

DIMETRA™

DIMETRA X Core

Core Server Restoration

Backup and Restore

System Release 9.1

MAY 2025

© 2025 Motorola Solutions, Inc. All Rights Reserved.



MN005731A01-E

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive



The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU and UK countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

© 2025 Motorola Solutions, Inc. All Rights Reserved

CMM Labeling and Disclosure Table

The People's Republic of China requires that our products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the Regulation Management Methods for Controlling Pollution by Electronic Information Products.) Two items are used to demonstrate compliance; the Label and the Disclosure Table.

The label is placed in a customer visible position on the product. The first of the following examples means that the product contains no hazardous substances; the second means that the product contains hazardous substances, and has an Environmental Friendly Use Period (EFUP) of fifty years.



The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution, or bodily injury from the use of the EIP.

The Disclosure Table, printed in simplified Chinese, is included with each customer order. An example of a Disclosure Table (in Chinese) follows:

Disclosure table

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr ⁶⁺)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件	×	○	×	×	○	○
电路模块	×	○	×	×	○	○
电缆及电缆组件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×

本表格依据 SJ/T 11364 的规定编制。
○: 表示该有毒有害物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。
×: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

Service Information

Technical & Repair Support (for Contracted Customers Only)

If you would like to contact the Motorola Solutions Customer Care team, use the appropriate contact details below. Please be prepared to provide your contract number, product serial numbers, and detailed issue description for a faster response and a resolution. If the support request is Technical Support related, the request will be handled by the Technical Support Operations (TSO) team. This team of highly skilled professionals provides Technical Support to help resolve technical issues and quickly restore networks and systems. If you are unsure whether your current service agreement entitles you to benefit from this service, or if you would like more information about the Technical or Repair Support Services, contact your local customer support or account manager for further information.

Contact Details

Technical Requests: techsupport.emea@motorolasolutions.com

Repair Support: repair.emea@motorolasolutions.com

Contact Us: https://www.motorolasolutions.com/en_xu/support.html

Parts Identification and Ordering

If you need help with identifying non-referenced spare parts, direct a request to the Customer Care Organization of a local area Motorola Solutions representative. Orders for replacement parts, kits, and assemblies should be placed directly at the local distribution organization of Motorola Solutions or through the Extranet site Motorola Online at <https://emeaonline.motorolasolutions.com>.

Document History

Version	Description	Date
MN005731A01-A	Initial version of the <i>Core Server Restoration</i> manual.	October 2019
MN005731A01-B	<p>Second version of the <i>Core Server Restoration</i> manual.</p> <p>Updates:</p> <ul style="list-style-type: none">● AS – Enabling the Application Server on page 141● AS – Installing Distinct ONC RPC License on page 138● MultiCADI – Installing Software Components on page 148 <p>Removed "AS – Disabling the Application Server"</p>	June 2020
MN005731A01-C	<p>Third version of the <i>Core Server Restoration</i> manual.</p> <p>Updates:</p> <ul style="list-style-type: none">● UCS – Collect and Combine on page 201● Server Restoration Prerequisites on page 37● Restoring Primary/Secondary Core Server Applications on page 39● Enabling All Application Servers on page 70● Air Traffic Router (ATR) – Software Application Restoration on page 126● MultiCADI – Software Application Restoration on page 146● MCADI – Restoring Data from Backup on page 150● MultiCADI – Restoring Application on page 146● MultiCADI – Network Security Software Installation on page 151● MultiCADI – AntiVirus Client Installation on page 151● MultiCADI – Application Configuration on page 148● UEM – Enabling the Application Server on page 223● Server Software Restoration on page 37● MultiCADI – Installing Software Components on page 148● Backing Up CRAM Configuration on page 304	October 2022

Version	Description	Date
	<ul style="list-style-type: none">● Restoring CRAM Service Configuration on page 308● Enabling the Read Permissions for CRAM SSL on page 308● Updating the License on Legacy Red Hat Anti-Virus Clients on page 71● Updating AntiVirus Client License by Using Enhanced Software Update Framework on page 72● Core Security Management Server – Software Application Restoration on page 83	
MN005731A01-D	Updates: <ul style="list-style-type: none">● ATR – Restoring Data from Backup on page 129● Loading Keys with Serial Connection on page 171	March 2025
MN005731A01-E	Updated section: <ul style="list-style-type: none">● Installing the External Modem Driver for KVL to AuC/PrC Communication on page 164	May 2025

Contents

Intellectual Property and Regulatory Notices	2
CMM Labeling and Disclosure Table	3
Service Information	4
Document History	5
List of Figures	20
List of Tables	21
List of Processes	23
List of Procedures	24
About Core Server Restoration	33
What Is Covered in This Manual?.....	33
Related Information.....	33
Icon Conventions	35
Style Conventions	36
Chapter 1: Server Software Restoration	37
1.1 Server Restoration Prerequisites.....	37
1.2 Obtaining the License Manager UUID.....	38
1.3 Restoring Primary/Secondary Core Server Applications.....	39
1.4 Service Redundancy Solution.....	42
1.4.1 Viewing Redundancy Information of a Device.....	42
1.4.2 Changing Redundancy State of a Device.....	43
1.4.3 Discovering Groups of Devices.....	44
1.4.4 Discovery Status.....	44
1.4.5 Redundancy State Window.....	45
1.5 Logging On to iGAS Through a Terminal Server.....	45
1.5.1 Messages Appearing when Establishing a Secure Session.....	46
1.6 Logging On to iGAS Through a KVM Switch.....	48
1.7 Checking the Installation Log.....	48
1.8 Checking RAID Configuration Status.....	49
1.9 Displaying iGAS Version and Server Information.....	49
1.10 Rebooting the Physical Server.....	50
1.11 Configuring Time Synchronization.....	51
1.11.1 Disabling Local Clock Monitor on Secondary Core Server.....	52
1.11.2 Synchronizing with Secondary Core Server.....	53
1.11.3 Enabling Local Clock Monitor on Secondary Core Server.....	55
1.11.4 Configuring Initial Time Service – Primary Core Server in the Lowest Zone Octet, Lowest Cluster Octet.....	56

1.11.5 Configuring Initial Time Service – Other Primary Core Servers.....	58
1.11.6 Configuring Initial Time Service – Secondary Core Server.....	59
1.11.7 Forcing Time Synchronization to the NTP Server.....	61
1.12 Configuring iLO Security.....	63
1.13 iLO Configuration Verification.....	63
1.13.1 Checking iLO License Status.....	63
1.14 License Manager Post-Restoration Operations.....	64
1.14.1 Verifying the License Manager UUID.....	64
1.14.2 Updating the License Manager UUID.....	65
1.14.2.1 Changing the License Manager UUID.....	65
1.14.3 Booting Primary/Secondary Core Server Application Servers.....	66
1.14.4 Enabling the Application Server.....	66
1.14.5 Uploading Licenses to the License Manager.....	67
1.15 Adding Zone to a Cluster.....	68
1.16 Enabling All Application Servers.....	70
1.17 Updating the License on Legacy Red Hat AntiVirus Clients.....	71
1.17.1 Updating AntiVirus Client License by Using Enhanced Software Update Framework.....	72
1.18 Server Password Change.....	73
1.18.1 Changing the Server Administrator Password.....	73
1.18.2 Changing the iLO User Password.....	74
1.19 Primary/Secondary Core Server – Installing and Configuring RSA Authentication Software.....	74
1.19.1 Installing and Configuring RSA Authentication Software on Linux Applications.....	74
1.19.2 Installing and Configuring RSA Authentication Software on Windows Applications.....	75
Chapter 2: Domain Controller – Software Application Restoration (Windows 2016).....	76
2.1 DC – Restoration Impact.....	76
2.2 DC – Restoring Application.....	76
2.3 DC – Performing Post-Restoration Operations.....	77
2.4 Determining FSMO Role Owner.....	77
2.5 Seizing FSMO Roles.....	78
2.6 Transferring FSMO Roles.....	78
2.7 Cleaning Up Metadata.....	79
2.8 Promoting Additional Domain Controllers.....	79
2.8.1 Password Requirements.....	80
2.9 Active Directory Status Verification.....	80
2.9.1 Running Dcdiag Tests.....	81
2.9.2 Verifying Replication Status.....	81
Chapter 3: Core Security Management Server – Software Application Restoration.....	83
3.1 CSMS – Pre-Restoration Checks.....	83
3.2 CSMS – Software Application Restoration Reference.....	83
3.3 CSMS – Restoring Software by Using a Switchover.....	84

3.4 CSMS – Restoring Application.....	84
3.5 CSMS – Switching Server to Active State.....	85
3.5.1 Administering the Active/Standby AV CSMS.....	85
3.5.2 Active/Standby AV CSMS Administration Commands.....	85
3.5.3 CSMS – Starting Up the ESU Application.....	86
3.5.4 CSMS – Uploading a Backup File to UIS.....	87
3.5.5 CSMS – Restoring Data from Backup.....	88
3.5.6 CSMS – Re-activating the Restored AV CSMS.....	88
3.5.7 CSMS – Installing and Configuring RSA Authentication Software.....	89
3.6 CSMS – Configuring the AntiVirus Server.....	89
3.7 CSMS – Data Backup.....	89
3.7.1 CSMS – Starting Up the ESU Application.....	89
3.7.2 CSMS – Configuring Backup.....	90
3.7.3 CSMS – Backing Up Data On-Demand.....	90
3.7.4 CSMS – Scheduling Backup.....	91
3.7.5 CSMS – Downloading a Backup File to the NM Client PC.....	92
Chapter 4: UIS – Software Application Restoration.....	93
4.1 UIS – Restoration Impact.....	93
4.2 UIS – Pre-Restoration Checks.....	94
4.3 UIS – Restoring Software.....	94
4.3.1 UIS – Restoring Application.....	94
4.3.2 UIS – Configuring Application.....	95
4.4 UIS – Restoring Data on a Redundant Master UIS.....	95
4.4.1 Checking Reinstalled Application Availability in ESU.....	95
4.4.2 Checking File Integrity.....	96
4.5 UIS – Restoring Data on Non-Redundant Master UIS.....	97
4.5.1 Uploading Files.....	97
4.5.2 Restoring a Database on a Non-Redundant Master UIS.....	98
4.6 UIS – Restoring Data on Zone UIS.....	99
4.6.1 Checking Reinstalled Application Availability in ESU.....	99
4.6.2 Checking File Integrity.....	99
4.7 Generating and Installing SSH Keys.....	101
4.8 UIS – Installing and Configuring RSA Authentication Software.....	101
4.9 UIS – Post-Restoration Checks.....	102
4.10 UIS – Backing Up Data.....	102
4.10.1 Starting Up the Upgrade Console.....	102
4.10.2 Configuring Backups.....	103
4.10.3 Backing Up the Master UIS.....	105
4.10.4 Scheduling Backups.....	106
4.10.5 Downloading Backup Files.....	107

Chapter 5: Zone Controller (ZC) Restoration.....	108
5.1 ZC – Restoration Impact.....	108
5.2 ZC – Pre-Restoration Checks.....	109
5.2.1 ZC – Checking Operational Status.....	109
5.2.1.1 ZC – Viewing Zone Controller System Status.....	109
5.2.1.1.1 ZC – Status Descriptions.....	110
5.2.1.1.2 ZC – Zone Database Server Status Descriptions.....	112
5.2.1.1.3 ZC – Operating Mode Descriptions.....	112
5.2.1.1.4 ZC – Requested Status Descriptions.....	112
5.3 ZC – Restoring Software.....	112
5.3.1 ZC – Restoring Application.....	113
5.3.2 ZC – Application Configuration.....	114
5.4 ZC – Restoring Data from Backup.....	114
5.4.1 ZC – Logging On to the Server.....	114
5.4.2 ZC – Disabling the Application Server.....	115
5.4.3 ZC – Restoring Data from Backup.....	115
5.4.4 ZC – Enabling the Application Server.....	116
5.5 Displaying Current KVL Assignment.....	116
5.6 Attaching KVL to Application.....	117
5.7 ZC – Installing and Configuring RSA Authentication Software.....	118
5.8 ZC – Post-Restoration Checks.....	118
5.8.1 ZC – Checking Operational Status.....	118
5.8.1.1 ZC – Viewing Zone Controller System Status.....	118
5.8.1.1.1 ZC – Status Descriptions.....	120
5.8.1.1.2 ZC – Zone Database Server Status Descriptions.....	121
5.8.1.1.3 ZC – Operating Mode Descriptions.....	121
5.8.1.1.4 ZC – Requested Status Descriptions.....	122
5.9 ZC – Backing Up Data.....	122
5.9.1 ZC – Starting Up the Upgrade Console.....	122
5.9.2 ZC – Configuring a Backup.....	122
5.9.3 ZC – Backing Up Data On-Demand.....	123
5.9.4 ZC – Scheduling Backup.....	124
5.9.5 ZC – Downloading a Backup File to the NM Client PC.....	125
Chapter 6: Air Traffic Router (ATR) – Software Application Restoration.....	126
6.1 ATR – Restoration Impact.....	126
6.2 ATR – Restoring Software.....	126
6.2.1 ATR – Restoring Application.....	126
6.2.2 ATR – Configuring Application.....	127
6.2.2.1 ATR – Enabling the Application Server.....	128
6.3 ATR – Restoring Data from Backup.....	129

6.4 UCS – Collect and Combine.....	129
6.5 ATR – Installing and Configuring RSA Authentication Software.....	131
6.6 ATR – Post-Restoration Checks.....	131
6.7 ATR – Backing Up Data.....	131
6.7.1 ATR – Starting Up the Upgrade Console.....	131
6.7.2 ATR – Configuring a Backup.....	132
6.7.3 ATR – Backing Up Data On-Demand.....	133
6.7.4 ATR – Scheduling Backup.....	133
6.7.5 ATR – Downloading a Backup File to the NM Client PC.....	134
Chapter 7: Alias Server – Software Application Restoration.....	136
7.1 AS – Restoration Impact.....	136
7.2 AS – Pre-Restoration Checks.....	136
7.3 AS – Restoring Software.....	137
7.3.1 AS – Restoring Application.....	137
7.3.2 AS – Configuring Application (Windows Server 2016 Procedures).....	138
7.3.2.1 AS – Installing Distinct ONC RPC License.....	138
7.3.2.2 Rebooting the Alias Server.....	138
7.4 AS – Restoring Data from Backup.....	139
7.4.1 AS – Starting Up the Upgrade Console.....	139
7.4.2 AS – Uploading a Backup File to UIS.....	139
7.4.3 Accessing Virtual Machines with the Web-Based Client.....	140
7.4.4 AS – Restoring Data from Backup.....	141
7.4.5 AS – Enabling the Application Server.....	141
7.5 AS – Installing and Configuring RSA Authentication Software.....	142
7.6 AS – Post-Restoration Checks.....	142
7.6.1 AS – Checking the AS Application.....	142
7.7 AS – Backing Up Data.....	143
7.7.1 AS – Starting Up the Upgrade Console.....	143
7.7.2 AS – Configuring a Backup.....	143
7.7.3 AS – Backing Up Data On-Demand.....	144
7.7.4 AS – Scheduling Backup.....	144
7.7.5 AS – Downloading a Backup File to the NM Client PC.....	145
Chapter 8: MultiCADI – Software Application Restoration.....	146
8.1 MultiCADI – Restoring Software.....	146
8.1.1 MultiCADI – Restoring Application.....	146
8.2 MultiCADI – Application Configuration.....	148
8.3 MCADI – Restoring Data from Backup.....	148
8.3.1 MultiCADI – Installing Software Components.....	148
8.3.2 MCADI – Enabling the Application Server.....	148
8.3.3 MCADI – Starting Up the Upgrade Console.....	149

8.3.4 MCADI – Uploading a Backup File to UIS.....	149
8.3.5 MCADI – Restoring Data from Backup.....	150
8.4 MultiCADI – Network Security Software Installation.....	151
8.4.1 MCADI – Installing and Configuring RSA Authentication Software.....	151
8.4.2 MultiCADI – AntiVirus Client Installation.....	151
8.5 MultiCADI – Post-Restoration Checks.....	151
8.5.1 MultiCADI – Checking the Configuration Tool.....	151
8.5.2 MultiCADI – Enabling the MultiCADI.....	152
8.5.3 MultiCADI – Checking the MultiCADI Application.....	152
8.6 MultiCADI – Backing Up Data.....	153
8.6.1 MultiCADI – Starting Up the Upgrade Console.....	153
8.6.2 MultiCADI – Configuring a Backup.....	153
8.6.3 MultiCADI – Backing Up Data On-Demand.....	154
8.6.4 MultiCADI – Scheduling Backup.....	155
8.6.5 MultiCADI – Downloading a Backup File to the NM Client PC.....	155
Chapter 9: Authentication Centre (AuC) Software Application Restoration.....	157
9.1 AuC – Restoration Impact.....	157
9.2 AuC – Pre-Restoration Checks.....	158
9.2.1 AuC – Checking Status of the Zone Controller.....	158
9.2.2 AuC – Recording the Key Version Numbers.....	159
9.2.3 AuC – Determining Key Version Numbers in AuC Backup File.....	160
9.2.4 AuC – Managing AuC Roles.....	160
9.2.4.1 Switching the Roles of the AuC Servers.....	160
9.2.4.1.1 Shutting Down Application Servers.....	161
9.2.4.2 Managing AuC Roles After Failure of Active AuC.....	161
9.2.4.3 Managing AuC Roles After Failure of Standby AuC.....	162
9.2.4.4 Changing the Role of the Standby AuC to Active AuC.....	162
9.3 AuC – Restoring Application.....	162
9.3.1 Installing the External Modem Driver for KVL to AuC/PrC Communication.....	164
9.4 AuC – Restoring Data from Backup.....	165
9.4.1 AuC – Starting Up the Upgrade Console.....	165
9.4.2 AuC – Uploading a Backup File to UIS.....	165
9.4.3 Accessing Virtual Machines with the Web-Based Client.....	166
9.4.4 AuC – Disabling the Application Server.....	167
9.4.5 AuC – Restoring Data from Backup.....	167
9.4.6 AuC – Enabling the Application Server.....	168
9.5 Replacing CryptR2.....	168
9.5.1 Displaying Current KVL Assignment.....	169
9.5.2 Attaching KVL to Application.....	169
9.5.3 Loading Keys with KVL.....	170

9.5.4 Loading Keys with Serial Connection.....	171
9.6 AuC – Configuring Application.....	172
9.6.1 AuC – Restoring Keys After a Database Restore.....	172
9.6.1.1 AuC – Restoring Keys on a Single Cluster AuC.....	172
9.6.1.2 AuC – Restoring Keys on a Master AuC.....	173
9.6.1.3 AuC – Restoring Keys on a Slave AuC.....	174
9.6.1.4 AuC – Restoring Keys Troubleshooting.....	175
9.6.2 AuC – Ensuring That the AuC Is Operational After Restoration.....	177
9.6.3 AuC – Cleaning Up the AuC Database.....	177
9.7 AuC – Installing and Configuring RSA Authentication Software.....	178
9.8 AuC – Post-Restoration Checks.....	178
9.9 AuC – Backup Procedures.....	179
9.9.1 AuC – Backing Up Data.....	179
9.9.1.1 AuC – Starting Up the Upgrade Console.....	179
9.9.1.2 AuC – Configuring a Backup.....	179
9.9.1.3 AuC – Backing Up Data On-Demand.....	180
9.9.1.4 AuC – Scheduling Backup.....	181
9.9.1.5 AuC – Downloading a Backup File to the NM Client PC.....	182
Chapter 10: System Statistics Server (SSS) – Software Application Restoration.....	183
10.1 SSS – Restoration Impact.....	183
10.2 SSS – Pre-Restoration Checks.....	183
10.2.1 SSS – Disabling the Application Server.....	184
10.3 SSS – Restoring Software.....	184
10.3.1 SSS – Restoring Application.....	184
10.3.2 SSS – Configuring Application.....	185
10.3.2.1 SSS – Enabling the Application Server.....	186
10.4 SSS – Restoring Data from Backup.....	186
10.4.1 SSS – Logging On to the Server.....	186
10.4.2 SSS – Disabling the Application Server.....	187
10.4.3 SSS – Restoring Data from Backup.....	187
10.4.4 SSS – Enabling the Application Server.....	188
10.5 SSS – Installing and Configuring RSA Authentication Software.....	189
10.6 SSS – Post-Restoration Checks.....	189
10.7 SSS – Backing Up Data.....	189
10.7.1 SSS – Starting Up the Upgrade Console.....	189
10.7.2 SSS – Configuring a Backup.....	190
10.7.3 SSS – Backing Up Data On-Demand.....	191
10.7.4 SSS – Scheduling Backup.....	191
10.7.5 SSS – Downloading a Backup File to the NM Client PC.....	192
Chapter 11: User Configuration Server (UCS) – Software Application Restoration.....	194

11.1 UCS – Restoration Impact.....	194
11.2 UCS – Pre-Restoration Checks.....	195
11.2.1 UCS – Disabling Application Server.....	195
11.3 UCS – Restoring Software.....	196
11.3.1 UCS – Restoring Application.....	196
11.3.2 UCS – Configuring Application.....	197
11.3.2.1 UCS – Enabling the Application Server.....	197
11.4 UCS – Restoring Data from Backup.....	198
11.4.1 UCS – Logging On to the Server.....	198
11.4.2 UCS – Disabling the Application Server.....	198
11.4.3 UCS – Restoring Data from Backup.....	199
11.4.4 UCS – Enabling the Application Server.....	199
11.5 UCS – Exporting Radio Control Manager Data.....	200
11.6 UCS – Collect and Combine.....	201
11.7 UCS – Installing and Configuring RSA Authentication Software.....	203
11.8 UCS – Post-Restoration Checks.....	203
11.8.1 ZDS – Disabling the Application Server.....	204
11.8.2 ZDS – Synchronizing Zone Database with UCS.....	204
11.8.3 ZDS – Checking SDR Database Synchronization.....	205
11.8.4 Enabling Application Servers.....	206
11.9 UCS – Backing Up Data.....	206
11.9.1 UCS – Starting Up the Upgrade Console.....	207
11.9.2 UCS – Configuring a Backup.....	207
11.9.3 UCS – Backing Up Data On-Demand.....	208
11.9.4 UCS – Scheduling Backup.....	208
11.9.5 UCS – Downloading a Backup File to the NM Client PC.....	209
Chapter 12: License Manager – Software Application Restoration.....	211
12.1 License Manager – Restoration Impact.....	211
12.2 License Manager – Pre-Restoration Checks.....	211
12.2.1 License Manager – Disabling Application Server.....	211
12.3 License Manager – Restoring Software.....	212
12.3.1 License Manager – Restoring Application.....	212
12.3.2 License Manager – Enabling the Application Server.....	213
12.4 License Manager – Restoring Data from Backup.....	214
12.4.1 License Manager – Disabling Application Server.....	214
12.4.2 License Manager – Restoring Data from Backup.....	214
12.4.3 License Manager – Enabling the Application Server.....	215
12.5 License Manager – Backing Up Data.....	216
12.5.1 License Manager – Starting Up the Upgrade Console.....	216
12.5.2 License Manager – Configuring a Backup.....	216

12.5.3 License Manager – Backing Up Data On-Demand.....	217
12.5.4 License Manager – Scheduling Backup.....	218
12.5.5 License Manager – Downloading a Backup File to the NM Client PC.....	218
Chapter 13: Unified Event Manager (UEM) – Software Application Restoration.....	220
13.1 UEM – Restoration Impact.....	220
13.2 UEM – Pre-Restoration Checks.....	220
13.2.1 UEM – Disabling Application Server.....	221
13.3 UEM – Restoring Software.....	221
13.3.1 UEM – Restoring Application.....	221
13.3.2 UEM – Configuring Application.....	223
13.3.2.1 UEM – Enabling the Application Server.....	223
13.4 UEM – Restoring Data from Backup.....	223
13.4.1 UEM – Logging On to the Server.....	223
13.4.2 UEM – Disabling the Application Server.....	224
13.4.3 UEM – Restoring Data from Backup.....	224
13.4.4 UEM – Enabling the Application Server.....	225
13.5 UEM – Installing and Configuring RSA Authentication Software.....	226
13.6 UEM – Post-Restoration Checks.....	226
13.7 UEM – Backing Up Data.....	226
13.7.1 UEM – Starting Up the Upgrade Console.....	227
13.7.2 UEM – Configuring a Backup.....	227
13.7.3 UEM – Backing Up Data On-Demand.....	228
13.7.4 UEM – Scheduling Backup.....	228
13.7.5 UEM – Downloading a Backup File to the NM Client PC.....	229
Chapter 14: Zone Database Server (ZDS) – Software Application Restoration.....	231
14.1 ZDS – Restoration Impact.....	231
14.2 ZDS – Pre-Restoration Checks.....	232
14.2.1 ZDS – Disabling Application Server.....	232
14.3 ZDS – Restoring Software.....	233
14.3.1 ZDS – Restoring Application.....	233
14.3.2 ZDS – Configuring Application.....	234
14.3.2.1 ZDS – Enabling the Application Server.....	234
14.3.2.2 ZDS – Synchronizing Zone Database with UCS.....	234
14.3.2.3 ZDS – Checking Data Replication Status.....	236
14.4 ZDS – Restoring Data from Backup.....	237
14.4.1 ZDS – Logging On to the Server.....	237
14.4.2 ZDS – Disabling the Application Server.....	238
14.4.3 ZDS – Restoring Data from Backup.....	238
14.4.4 ZDS – Enabling the Application Server.....	239
14.4.5 ZDS – Verifying Zone Controller Redundancy.....	239

14.5 ZDS – Installing and Configuring RSA Authentication Software.....	240
14.6 ZDS – Post-Restoration Checks.....	240
14.6.1 Downloading SAC to the ZCs.....	241
14.7 ZDS – Backing Up Data.....	241
14.7.1 ZDS – Starting Up the Upgrade Console.....	241
14.7.2 ZDS – Configuring a Backup.....	242
14.7.3 ZDS – Backing Up Data On-Demand.....	242
14.7.4 ZDS – Scheduling Backup.....	243
14.7.5 ZDS – Downloading a Backup File to the NM Client PC.....	244
Chapter 15: Zone Statistics Server (ZSS) – Software Application Restoration.....	245
15.1 ZSS – Restoration Impact.....	245
15.2 ZSS – Pre-Restoration Checks.....	245
15.2.1 ZSS – Disabling the Application Server.....	246
15.3 ZSS – Restoring Software.....	247
15.3.1 ZSS – Restoring Application.....	247
15.3.2 ZSS – Configuring Application.....	248
15.3.2.1 ZSS – Enabling the Application Server.....	248
15.4 ZSS – Restoring Data from Backup.....	249
15.4.1 ZSS – Logging On to the Server.....	249
15.4.2 ZSS – Disabling the Application Server.....	250
15.4.3 ZSS – Restoring Data from Backup.....	250
15.4.4 ZSS – Enabling the Application Server.....	251
15.5 ZSS – Installing and Configuring RSA Authentication Software.....	252
15.6 ZSS – Post-Restoration Checks.....	252
15.7 ZSS – Backing Up Data.....	252
15.7.1 ZSS – Starting Up the Upgrade Console.....	252
15.7.2 ZSS – Configuring a Backup.....	253
15.7.3 ZSS – Backing Up Data On-Demand.....	253
15.7.4 ZSS – Scheduling Backup.....	254
15.7.5 ZSS – Downloading a Backup File to the NM Client PC.....	255
Chapter 16: MTIG-IP Restoration.....	256
16.1 MTIG-IP – Restoration Impact.....	256
16.2 MTIG-IP – Pre-Restoration Checks.....	256
16.3 MTIG-IP – Restoring Software.....	257
16.3.1 MTIG-IP – Restoring Application.....	257
16.3.2 MTIG-IP – Configuring Application.....	258
16.3.2.1 Configuring the Host Based Firewall Rules.....	258
16.4 MTIG-IP – Restoring Data from Backup.....	259
16.4.1 MTIG-IP – Starting Up the Upgrade Console.....	259
16.4.2 MTIG-IP – Uploading a Backup File to UIS.....	260

16.4.3 MTIG-IP – Logging On to the Server.....	261
16.4.4 MTIG-IP – Disabling the Application Server.....	261
16.4.5 MTIG-IP – Restoring Data from Backup.....	262
16.4.6 MTIG-IP – Enabling the Application Server.....	262
16.5 MTIG-IP – Installing and Configuring RSA Authentication Software.....	263
16.6 MTIG-IP – Post-Restoration Checks.....	263
16.7 MTIG-IP – Backing Up Data.....	263
16.7.1 MTIG-IP – Starting Up the Upgrade Console.....	263
16.7.2 MTIG-IP – Configuring a Backup.....	264
16.7.3 MTIG-IP – Backing Up Data On-Demand.....	265
16.7.4 MTIG-IP – Scheduling Backup.....	265
16.7.5 MTIG-IP – Downloading a Backup File to the NM Client PC.....	266
16.8 Rebooting the MTIG-IP Server.....	267
Chapter 17: Data Subsystem Restoration.....	268
17.1 Packet Data Gateway (PDG) – Software Application Restoration.....	268
17.1.1 PDG – Restoration References.....	268
17.1.2 PDG – Restoration Impact.....	269
17.1.3 PDG – Pre-Restoration Checks.....	269
17.1.4 PDG – Restoring Software.....	269
17.1.4.1 PDR – Restoring Application.....	269
17.1.4.2 RNG – Restoring Application.....	270
17.1.5 PDG – Configuring Application.....	271
17.1.6 PDG – Restoring Data from Backup.....	271
17.1.6.1 PDG – Starting Up the Upgrade Console.....	271
17.1.6.2 PDG – Uploading a Backup File to UIS.....	272
17.1.6.3 PDG – Logging On to the Server.....	272
17.1.6.4 PDG – Restoring Data from Backup.....	273
17.1.7 PDG – Installing and Configuring RSA Authentication Software.....	274
17.1.8 PDG – Post-Restoration Checks.....	274
17.1.8.1 PDG – Checking Database Synchronization.....	275
17.1.8.2 PDR – Checking Synchronization Between the Active PDR and the Standby PDR.....	276
17.1.9 PDG – Backing Up Data.....	277
17.1.9.1 PDG – Starting Up the Upgrade Console.....	277
17.1.9.2 PDG – Configuring a Backup.....	277
17.1.9.3 PDR – Backing up Data On-Demand.....	278
17.1.9.4 PDG – Scheduling Backup.....	279
17.1.9.5 PDG – Downloading a Backup File to the NM Client PC.....	280
17.2 Short Data Router (SDR) – Software Application Restoration.....	280
17.2.1 SDR – Restoration References.....	280
17.2.2 SDR – Restoration Impact.....	281

17.2.3 SDR – Pre-Restoration Checks.....	281
17.2.4 SDR – Restoring Software.....	281
17.2.4.1 SDR – Restoring Application.....	281
17.2.5 SDR – Configuring Application.....	282
17.2.6 SDR – Restoring Data from Backup.....	283
17.2.6.1 SDR – Starting Up the Upgrade Console.....	283
17.2.6.2 SDR – Uploading a Backup File to UIS.....	283
17.2.6.3 SDR – Logging On to the Server.....	284
17.2.6.4 SDR – Restoring Data from Backup.....	285
17.2.7 SDR – Installing and Configuring RSA Authentication Software.....	285
17.2.8 SDR – Post-Restoration Checks.....	286
17.2.8.1 SDR – Checking SDR Database Synchronization.....	286
17.2.8.2 SDR – Verifying the Active-Standby SDR Synchronization.....	286
17.2.9 SDR – Backing Up Data.....	287
17.2.9.1 SDR – Starting Up the Upgrade Console.....	287
17.2.9.2 SDR – Configuring a Backup.....	287
17.2.9.3 SDR – Backing Up Data On-Demand.....	288
17.2.9.4 SDR – Scheduling Backup.....	289
17.2.9.5 SDR – Downloading a Backup File to the NM Client PC.....	290

Chapter 18: MCC 7500 Dispatch Communications Server (DCS) Subsystem Restoration 291

18.1 Audio Gateway (AGTW) Software Application Restoration.....	291
18.1.1 AGTW – Restoration Impact.....	291
18.1.2 AGTW – Pre-Restoration Checks.....	291
18.1.3 AGTW – Restoring Software.....	292
18.1.3.1 AGTW – Restoring Application.....	292
18.1.3.2 AGTW – Application Configuration.....	293
18.1.4 AGTW – Restoring Data from Backup.....	293
18.1.4.1 AGTW – Starting Up the Upgrade Console.....	293
18.1.4.2 AGTW – Uploading a Backup File to UIS.....	294
18.1.4.3 AGTW – Logging On to the Server.....	294
18.1.4.4 AGTW – Disabling the Application Server.....	295
18.1.4.5 AGTW – Restoring Data from Backup.....	295
18.1.4.6 AGTW – Enabling the Application Server.....	296
18.1.5 AGTW – Installing and Configuring RSA Authentication Software.....	297
18.1.6 AGTW – Post-Restoration Checks.....	297
18.1.7 AGTW – Backing Up Data.....	297
18.1.7.1 AGTW – Starting Up the Upgrade Console.....	298
18.1.7.2 AGTW – Configuring a Backup.....	298
18.1.7.3 AGTW – Backing Up Data On-Demand.....	299
18.1.7.4 AGTW – Scheduling Backup.....	300

18.1.7.5 AGTW – Downloading a Backup File to the NM Client PC.....	300
18.2 Call Control Entity (CCE) Software Application Restoration	301
18.2.1 CCE – Restoration Impact.....	301
18.2.2 CCE – Pre-Restoration Checks.....	302
18.2.3 CCE – Restoring Software.....	302
18.2.3.1 CCE – Application Configuration.....	302
18.2.3.2 CCE – Restoring Application.....	303
18.2.4 Backing Up CRAM Configuration.....	304
18.2.5 CCE – Restoring Data from Backup.....	305
18.2.5.1 CCE – Starting Up the Upgrade Console.....	305
18.2.5.2 CCE – Uploading a Backup File to UIS.....	305
18.2.5.3 CCE – Logging On to the Server.....	306
18.2.5.4 CCE – Disabling the Application Server.....	307
18.2.5.5 CCE – Restoring Data from Backup.....	307
18.2.5.6 Restoring CRAM Service Configuration.....	308
18.2.5.7 Enabling the Read Permissions for CRAM SSL.....	308
18.2.5.8 CCE – Enabling the Application Server.....	309
18.2.6 CCE – Installing and Configuring RSA Authentication Software.....	309
18.2.7 CCE – Verifying Service Startup Type.....	310
18.2.7.1 Accessing Virtual Machines with the Web-Based Client.....	310
18.2.8 CCE – Post-Restoration Checks.....	311
18.2.9 CCE – Backing Up Data.....	311
18.2.9.1 CCE – Starting Up the Upgrade Console.....	311
18.2.9.2 CCE – Configuring a Backup.....	312
18.2.9.3 CCE – Backing Up Data On-Demand.....	313
18.2.9.4 CCE – Scheduling Backup.....	313
18.2.9.5 CCE – Downloading a Backup File to the NM Client PC.....	314

List of Figures

Figure 1: Server Restoration Process Documentation Map.....	37
Figure 2: Upload Licenses Button.....	68
Figure 3: Change Report Window.....	68
Figure 4: Replication Status Log.....	81
Figure 5: File Integrity Page.....	96
Figure 6: Check Integrity Page – Integrity Check in Progress.....	97
Figure 7: File Integrity Page.....	100
Figure 8: Check Integrity Page – Integrity Check in Progress.....	100
Figure 9: Backup Configuration Page.....	104
Figure 10: New Backup Schedule Page.....	106
Figure 11: OTAR Keys Handling Group Box.....	176
Figure 12: PDR – Local Configuration Main Menu.....	276
Figure 13: PDR – Database Synchronization Screen.....	276

List of Tables

Table 1: Core Server Restoration Prerequisites.....	37
Table 2: Parameters for the Redundancy State Window.....	45
Table 3: Messages Appearing when Establishing a Secure Session.....	47
Table 4: Primary/Secondary Core Server – Time Synchronization.....	51
Table 5: NTP Servers Administration Menu – Settings.....	62
Table 6: Core Security Management Server – Restoration Reference.....	83
Table 7: Administrator: Manage CSMS – Commands.....	85
Table 8: UIS – Backup and Restoration Checklist.....	93
Table 9: UIS – Restoration Impact.....	93
Table 10: ZC - Restoration References.....	108
Table 11: ZC – Restoration Impact.....	108
Table 12: ZC – Pre-Restoration Checks.....	109
Table 13: Zone Controller Status Descriptions.....	110
Table 14: ZC – Zone Database Server Statuses.....	112
Table 15: ZC – Zone Controller Operating Mode Descriptions.....	112
Table 16: ZC – Zone Controller Requested Status Descriptions.....	112
Table 17: ZC – Post-Restoration Checks.....	118
Table 18: Zone Controller Status Descriptions.....	120
Table 19: ZC – Zone Database Server Statuses.....	121
Table 20: ZC – Zone Controller Operating Mode Descriptions.....	121
Table 21: ZC – Zone Controller Requested Status Descriptions.....	122
Table 22: ATR – Restoration References.....	126
Table 23: ATR – Restoration Impact.....	126
Table 24: ATR – Post-Restoration Checks.....	131
Table 25: Alias Server – Restoration Reference.....	136
Table 26: Alias Server – Restoration Impact.....	136
Table 27: AS – Restoration Prerequisites.....	136
Table 28: AS – Post-Restoration Checks.....	142
Table 29: MultiCADI – Restoration References.....	146
Table 30: AuC – Restoration References.....	157
Table 31: AuC – Restoration Impact.....	157
Table 32: AuC – Pre-Restoration Checks.....	158
Table 33: AuC – Post-Restoration Checks.....	178
Table 34: SSS – Restoration References.....	183
Table 35: SSS – Restoration Impact.....	183
Table 36: SSS – Pre-Restoration Checks.....	183

Table 37: SSS – Post-restoration Checks.....	189
Table 38: User Configuration Server – Restoration References.....	194
Table 39: UCS – Restoration Impact.....	194
Table 40: UCS – Pre-Restoration Checks.....	195
Table 41: UCS – Post-Restoration Checks.....	203
Table 42: License Manager – Restoration Impact.....	211
Table 43: License Manager – Pre-Restoration Checks.....	211
Table 44: Unified Event Manager – Restoration References.....	220
Table 45: UEM – Restoration Impact.....	220
Table 46: UEM – Pre-Restoration Checks.....	220
Table 47: UEM – Post-Restoration Checks.....	226
Table 48: Zone Database Server – Restoration References.....	231
Table 49: ZDS – Restoration Impact.....	231
Table 50: ZDS – Pre-Restoration Checks.....	232
Table 51: ZDS – Post-Restoration Checks.....	240
Table 52: Zone Statistics Server – Restoration References.....	245
Table 53: ZSS – Restoration Impact.....	245
Table 54: ZSS – Pre-Restoration Checks.....	245
Table 55: ZSS – Post-Restoration Checks.....	252
Table 56: MTIG-IP – Backup and Restoration Checklist.....	256
Table 57: MTIG-IP – Restoration Impact.....	256
Table 58: PDG – Restoration References.....	268
Table 59: PDG – Restoration Impact.....	269
Table 60: PDG – Post-Restoration Checks.....	274
Table 61: SDR – Restoration References.....	281
Table 62: SDR – Restoration Impact.....	281
Table 63: SDR – Post-Restoration Checks.....	286
Table 64: Audio Gateway (AGTW) Server – Backup and Restoration Checklist.....	291
Table 65: AGTW – Restoration Impact.....	291
Table 66: Call Control Entity (CCE) Server – Backup and Restoration Checklist.....	301
Table 67: CCE – Restoration Impact.....	301
Table 68: CRAM SSL–Certificate Files to Back Up.....	304

List of Processes

Configuring Time Synchronization	51
License Manager Post-Restoration Operations	64
Updating the License Manager UUID	65
DC – Performing Post-Restoration Operations	77
CSMS – Restoring Software by Using a Switchover	84
CCE – Post-Restoration Checks	311

List of Procedures

Obtaining the License Manager UUID	38
Restoring Primary/Secondary Core Server Applications	39
Viewing Redundancy Information of a Device	42
Changing Redundancy State of a Device	43
Discovering Groups of Devices	44
Logging On to iGAS Through a Terminal Server	45
Logging On to iGAS Through a KVM Switch	48
Checking the Installation Log	48
Checking RAID Configuration Status	49
Displaying iGAS Version and Server Information	49
Rebooting the Physical Server	50
Disabling Local Clock Monitor on Secondary Core Server	52
Synchronizing with Secondary Core Server	53
Enabling Local Clock Monitor on Secondary Core Server	55
Configuring Initial Time Service – Primary Core Server in the Lowest Zone Octet, Lowest Cluster Octet	56
Configuring Initial Time Service – Other Primary Core Servers	58
Configuring Initial Time Service – Secondary Core Server	59
Forcing Time Synchronization to the NTP Server	61
Configuring iLO Security	63
Checking iLO License Status	63
Verifying the License Manager UUID	64
Changing the License Manager UUID	65
Booting Primary/Secondary Core Server Application Servers	66
Enabling the Application Server	66
Uploading Licenses to the License Manager	67
Adding Zone to a Cluster	68
Enabling All Application Servers	70
Updating the License on Legacy Red Hat AntiVirus Clients	71
Updating AntiVirus Client License by Using Enhanced Software Update Framework	72
Changing the Server Administrator Password	73
Changing the iLO User Password	74
Installing and Configuring RSA Authentication Software on Linux Applications	74
Installing and Configuring RSA Authentication Software on Windows Applications	75
DC – Restoring Application	76
Determining FSMO Role Owner	77
Seizing FSMO Roles	78

Transferring FSMO Roles	78
Cleaning Up Metadata	79
Promoting Additional Domain Controllers	79
Running Dcdiag Tests	81
Verifying Replication Status	81
CSMS – Restoring Application	84
CSMS – Switching Server to Active State	85
Administering the Active/Standby AV CSMS	85
CSMS – Starting Up the ESU Application	86
CSMS – Uploading a Backup File to UIS	87
CSMS – Restoring Data from Backup	88
CSMS – Re-activating the Restored AV CSMS	88
CSMS – Installing and Configuring RSA Authentication Software	89
CSMS – Configuring the AntiVirus Server	89
CSMS – Starting Up the ESU Application	89
CSMS – Configuring Backup	90
CSMS – Backing Up Data On-Demand	90
CSMS – Scheduling Backup	91
CSMS – Downloading a Backup File to the NM Client PC	92
UIS – Restoring Application	94
Checking Reinstalled Application Availability in ESU	95
Checking File Integrity	96
Uploading Files	97
Restoring a Database on a Non-Redundant Master UIS	98
Checking Reinstalled Application Availability in ESU	99
Checking File Integrity	99
Generating and Installing SSH Keys	101
UIS – Installing and Configuring RSA Authentication Software	101
Starting Up the Upgrade Console	102
Configuring Backups	103
Backing Up the Master UIS	105
Scheduling Backups	106
Downloading Backup Files	107
ZC – Viewing Zone Controller System Status	109
ZC – Restoring Application	113
ZC – Logging On to the Server	114
ZC – Disabling the Application Server	115
ZC – Restoring Data from Backup	115
ZC – Enabling the Application Server	116

Displaying Current KVL Assignment	116
Attaching KVL to Application	117
ZC – Installing and Configuring RSA Authentication Software	118
ZC – Viewing Zone Controller System Status	118
ZC – Starting Up the Upgrade Console	122
ZC – Configuring a Backup	122
ZC – Backing Up Data On-Demand	123
ZC – Scheduling Backup	124
ZC – Downloading a Backup File to the NM Client PC	125
ATR – Restoring Application	126
ATR – Enabling the Application Server	128
ATR – Restoring Data from Backup	129
UCS – Collect and Combine	129
ATR – Installing and Configuring RSA Authentication Software	131
ATR – Starting Up the Upgrade Console	131
ATR – Configuring a Backup	132
ATR – Backing Up Data On-Demand	133
ATR – Scheduling Backup	133
ATR – Downloading a Backup File to the NM Client PC	134
AS – Restoring Application	137
AS – Installing Distinct ONC RPC License	138
Rebooting the Alias Server	138
AS – Starting Up the Upgrade Console	139
AS – Uploading a Backup File to UIS	139
Accessing Virtual Machines with the Web-Based Client	140
AS – Restoring Data from Backup	141
AS – Enabling the Application Server	141
AS – Installing and Configuring RSA Authentication Software	142
AS – Starting Up the Upgrade Console	143
AS – Configuring a Backup	143
AS – Backing Up Data On-Demand	144
AS – Scheduling Backup	144
AS – Downloading a Backup File to the NM Client PC	145
MultiCADI – Restoring Application	146
MultiCADI – Installing Software Components	148
MCADI – Enabling the Application Server	148
MCADI – Starting Up the Upgrade Console	149
MCADI – Uploading a Backup File to UIS	149
MCADI – Restoring Data from Backup	150

MCADI – Installing and Configuring RSA Authentication Software	151
MultiCADI – Enabling the MultiCADI	152
MultiCADI – Starting Up the Upgrade Console	153
MultiCADI – Configuring a Backup	153
MultiCADI – Backing Up Data On-Demand	154
MultiCADI – Scheduling Backup	155
MultiCADI – Downloading a Backup File to the NM Client PC	155
AuC – Checking Status of the Zone Controller	158
AuC – Recording the Key Version Numbers	159
AuC – Determining Key Version Numbers in AuC Backup File	160
Switching the Roles of the AuC Servers	160
Shutting Down Application Servers	161
Changing the Role of the Standby AuC to Active AuC	162
AuC – Restoring Application	162
Installing the External Modem Driver for KVL to AuC/PrC Communication	164
AuC – Starting Up the Upgrade Console	165
AuC – Uploading a Backup File to UIS	165
Accessing Virtual Machines with the Web-Based Client	166
AuC – Disabling the Application Server	167
AuC – Restoring Data from Backup	167
AuC – Enabling the Application Server	168
Replacing CryptR2	168
Displaying Current KVL Assignment	169
Attaching KVL to Application	169
Loading Keys with KVL	170
Loading Keys with Serial Connection	171
AuC – Restoring Keys on a Single Cluster AuC	172
AuC – Restoring Keys on a Master AuC	173
AuC – Restoring Keys on a Slave AuC	174
AuC – Restoring Keys Troubleshooting	175
AuC – Ensuring That the AuC Is Operational After Restoration	177
AuC – Cleaning Up the AuC Database	177
AuC – Installing and Configuring RSA Authentication Software	178
AuC – Starting Up the Upgrade Console	179
AuC – Configuring a Backup	179
AuC – Backing Up Data On-Demand	180
AuC – Scheduling Backup	181
AuC – Downloading a Backup File to the NM Client PC	182
SSS – Disabling the Application Server	184

SSS – Restoring Application	184
SSS – Enabling the Application Server	186
SSS – Logging On to the Server	186
SSS – Disabling the Application Server	187
SSS – Restoring Data from Backup	187
SSS – Enabling the Application Server	188
SSS – Installing and Configuring RSA Authentication Software	189
SSS – Starting Up the Upgrade Console	189
SSS – Configuring a Backup	190
SSS – Backing Up Data On-Demand	191
SSS – Scheduling Backup	191
SSS – Downloading a Backup File to the NM Client PC	192
UCS – Disabling Application Server	195
UCS – Restoring Application	196
UCS – Enabling the Application Server	197
UCS – Logging On to the Server	198
UCS – Disabling the Application Server	198
UCS – Restoring Data from Backup	199
UCS – Enabling the Application Server	199
UCS – Exporting Radio Control Manager Data	200
UCS – Collect and Combine	201
UCS – Installing and Configuring RSA Authentication Software	203
ZDS – Disabling the Application Server	204
ZDS – Synchronizing Zone Database with UCS	204
ZDS – Checking SDR Database Synchronization	205
Enabling Application Servers	206
UCS – Starting Up the Upgrade Console	207
UCS – Configuring a Backup	207
UCS – Backing Up Data On-Demand	208
UCS – Scheduling Backup	208
UCS – Downloading a Backup File to the NM Client PC	209
License Manager – Disabling Application Server	211
License Manager – Restoring Application	212
License Manager – Enabling the Application Server	213
License Manager – Disabling Application Server	214
License Manager – Restoring Data from Backup	214
License Manager – Enabling the Application Server	215
License Manager – Starting Up the Upgrade Console	216
License Manager – Configuring a Backup	216

License Manager – Backing Up Data On-Demand	217
License Manager – Scheduling Backup	218
License Manager – Downloading a Backup File to the NM Client PC	218
UEM – Disabling Application Server	221
UEM – Restoring Application	221
UEM – Enabling the Application Server	223
UEM – Logging On to the Server	223
UEM – Disabling the Application Server	224
UEM – Restoring Data from Backup	224
UEM – Enabling the Application Server	225
UEM – Installing and Configuring RSA Authentication Software	226
UEM – Starting Up the Upgrade Console	227
UEM – Configuring a Backup	227
UEM – Backing Up Data On-Demand	228
UEM – Scheduling Backup	228
UEM – Downloading a Backup File to the NM Client PC	229
ZDS – Disabling Application Server	232
ZDS – Restoring Application	233
ZDS – Enabling the Application Server	234
ZDS – Synchronizing Zone Database with UCS	234
ZDS – Checking Data Replication Status	236
ZDS – Logging On to the Server	237
ZDS – Disabling the Application Server	238
ZDS – Restoring Data from Backup	238
ZDS – Enabling the Application Server	239
ZDS – Verifying Zone Controller Redundancy	239
ZDS – Installing and Configuring RSA Authentication Software	240
Downloading SAC to the ZCs	241
ZDS – Starting Up the Upgrade Console	241
ZDS – Configuring a Backup	242
ZDS – Backing Up Data On-Demand	242
ZDS – Scheduling Backup	243
ZDS – Downloading a Backup File to the NM Client PC	244
ZSS – Disabling the Application Server	246
ZSS – Restoring Application	247
ZSS – Enabling the Application Server	248
ZSS – Logging On to the Server	249
ZSS – Disabling the Application Server	250
ZSS – Restoring Data from Backup	250

ZSS – Enabling the Application Server	251
ZSS – Installing and Configuring RSA Authentication Software	252
ZSS – Starting Up the Upgrade Console	252
ZSS – Configuring a Backup	253
ZSS – Backing Up Data On-Demand	253
ZSS – Scheduling Backup	254
ZSS – Downloading a Backup File to the NM Client PC	255
MTIG-IP – Restoring Application	257
Configuring the Host Based Firewall Rules	258
MTIG-IP – Starting Up the Upgrade Console	259
MTIG-IP – Uploading a Backup File to UIS	260
MTIG-IP – Logging On to the Server	261
MTIG-IP – Disabling the Application Server	261
MTIG-IP – Restoring Data from Backup	262
MTIG-IP – Enabling the Application Server	262
MTIG-IP – Installing and Configuring RSA Authentication Software	263
MTIG-IP – Starting Up the Upgrade Console	263
MTIG-IP – Configuring a Backup	264
MTIG-IP – Backing Up Data On-Demand	265
MTIG-IP – Scheduling Backup	265
MTIG-IP – Downloading a Backup File to the NM Client PC	266
Rebooting the MTIG-IP Server	267
PDR – Restoring Application	269
RNG – Restoring Application	270
PDG – Configuring Application	271
PDG – Starting Up the Upgrade Console	271
PDG – Uploading a Backup File to UIS	272
PDG – Logging On to the Server	272
PDG – Restoring Data from Backup	273
PDG – Installing and Configuring RSA Authentication Software	274
PDG – Checking Database Synchronization	275
PDR – Checking Synchronization Between the Active PDR and the Standby PDR	276
PDG – Starting Up the Upgrade Console	277
PDG – Configuring a Backup	277
PDR – Backing up Data On-Demand	278
PDG – Scheduling Backup	279
PDG – Downloading a Backup File to the NM Client PC	280
SDR – Restoring Application	281
SDR – Configuring Application	282

SDR – Starting Up the Upgrade Console	283
SDR – Uploading a Backup File to UIS	283
SDR – Logging On to the Server	284
SDR – Restoring Data from Backup	285
SDR – Installing and Configuring RSA Authentication Software	285
SDR – Checking SDR Database Synchronization	286
SDR – Verifying the Active-Standby SDR Synchronization	286
SDR – Starting Up the Upgrade Console	287
SDR – Configuring a Backup	287
SDR – Backing Up Data On-Demand	288
SDR – Scheduling Backup	289
SDR – Downloading a Backup File to the NM Client PC	290
AGTW – Restoring Application	292
AGTW – Starting Up the Upgrade Console	293
AGTW – Uploading a Backup File to UIS	294
AGTW – Logging On to the Server	294
AGTW – Disabling the Application Server	295
AGTW – Restoring Data from Backup	295
AGTW – Enabling the Application Server	296
AGTW – Installing and Configuring RSA Authentication Software	297
AGTW – Post-Restoration Checks	297
AGTW – Starting Up the Upgrade Console	298
AGTW – Configuring a Backup	298
AGTW – Backing Up Data On-Demand	299
AGTW – Scheduling Backup	300
AGTW – Downloading a Backup File to the NM Client PC	300
CCE – Pre-Restoration Checks	302
CCE – Restoring Application	303
Backing Up CRAM Configuration	304
CCE – Starting Up the Upgrade Console	305
CCE – Uploading a Backup File to UIS	305
CCE – Logging On to the Server	306
CCE – Disabling the Application Server	307
CCE – Restoring Data from Backup	307
Restoring CRAM Service Configuration	308
Enabling the Read Permissions for CRAM SSL	308
CCE – Enabling the Application Server	309
CCE – Installing and Configuring RSA Authentication Software	309
CCE – Verifying Service Startup Type	310

Accessing Virtual Machines with the Web-Based Client	310
CCE – Starting Up the Upgrade Console	311
CCE – Configuring a Backup	312
CCE – Backing Up Data On-Demand	313
CCE – Scheduling Backup	313
CCE – Downloading a Backup File to the NM Client PC	314

About Core Server Restoration

This manual describes how to perform restoration of the Primary/Secondary Core Server, including hardware, software, and data restoration of all application servers.

What Is Covered in This Manual?

This manual contains the following chapters:

- [Server Software Restoration on page 37](#)
- [Domain Controller – Software Application Restoration \(Windows 2016\) on page 76](#)
- [Core Security Management Server – Software Application Restoration on page 83](#)
- [UIS – Software Application Restoration on page 93](#)
- [Zone Controller \(ZC\) Restoration on page 108](#)
- [Air Traffic Router \(ATR\) – Software Application Restoration on page 126](#)
- [Alias Server – Software Application Restoration on page 136](#)
- [MultiCADI – Software Application Restoration on page 146](#)
- [Authentication Centre \(AuC\) Software Application Restoration on page 157](#)
- [System Statistics Server \(SSS\) – Software Application Restoration on page 183](#)
- [User Configuration Server \(UCS\) – Software Application Restoration on page 194](#)
- [License Manager – Software Application Restoration on page 211](#)
- [Unified Event Manager \(UEM\) – Software Application Restoration on page 220](#)
- [Zone Database Server \(ZDS\) – Software Application Restoration on page 231](#)
- [Zone Statistics Server \(ZSS\) – Software Application Restoration on page 245](#)
- [MTIG-IP Restoration on page 256](#)
- [Data Subsystem Restoration on page 268](#)
- [MCC 7500 Dispatch Communications Server \(DCS\) Subsystem Restoration on page 291](#)

Related Information

Document Title	Description
<i>Glossary</i>	The glossary provides definitions of terms, abbreviations, and acronyms used in the DIMETRA system documentation.
<i>Documentation Overview</i>	This document provides a list of all documents delivered with your DIMETRA system.
<i>System Overview</i>	This manual explains basic radio system concepts, call processing basics, and an introduction to the various components and processes associated with the DIMETRA system. The manual provides the background needed to comprehend DIMETRA system theory of operation. It also provides functional descriptions of

Document Title	Description
	equipment and subsystems, and describes the role of the numerous network management software applications used in the system.
<i>Enhanced Software Update User Guide</i>	This manual describes the Enhanced Software Update feature, which provides backup and restore functionality, and upgrade functionality.
<i>Network Management Client</i>	This manual provides an introduction to the hardware and software components associated with the Network Management (NM) Client. Detailed procedures for installation, configuration and operation are included.
<i>Network Security</i>	This manual describes all necessary actions to install, configure and maintain the network security feature within the DIMETRA system. The intention of the manual is to enable the reader to deploy the best possible level of security, which will protect the system against viruses, unauthorized authentication or attacks of hackers. The network security feature provides virus protection, authentication, and firewall protection.
<i>Zone Controller</i>	This manual describes the Zone Controller which is responsible for processing calls, managing audio paths, controlling zone infrastructure, and providing services to subscribers and console operators.
<i>HP ProLiant Gen9 Server Platform Restoration</i>	This manual describes how to restore a Gen9 server platform in case of a failure.
<i>Common Server and Client Platform Restoration</i>	This manual describes how to restore a Gen10 server platform in case of a failure. It contains information on replacing the hardware, as well as RAID/BIOS/iLO configuration.
<i>Performance and Security Management Server Restoration</i>	This manual explains how to restore the Performance and Security Management applications and the underlying server platform.
<i>Call Processing and Mobility Management</i>	This manual describes radio features and their configuration. The manual contains a configuration checklist as well as configuration procedures for the key features of the system.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set.

-  **DANGER:** The signal word DANGER with the associated safety icon implies information that, if disregarded, will result in death or serious injury.
-  **WARNING:** The signal word WARNING with the associated safety icon implies information that, if disregarded, could result in death or serious injury, or serious product damage.
-  **CAUTION:** The signal word CAUTION with the associated safety icon implies information that, if disregarded, may result in minor or moderate injury, or serious product damage.
- CAUTION:** The signal word CAUTION may be used without the safety icon to state potential damage or injury that is not related to the product.
-  **IMPORTANT:** IMPORTANT statements contain information that is crucial to the discussion at hand, but is not CAUTION or WARNING. There is no warning level associated with the IMPORTANT statement.
-  **NOTE:** NOTICE contains information more important than the surrounding text, such as exceptions or preconditions. They also refer the reader elsewhere for additional information, remind the reader how to complete an action (when it is not part of the current procedure, for instance), or tell the reader where something is on the screen. There is no warning level associated with a notice.

Style Conventions

The following style conventions are used:

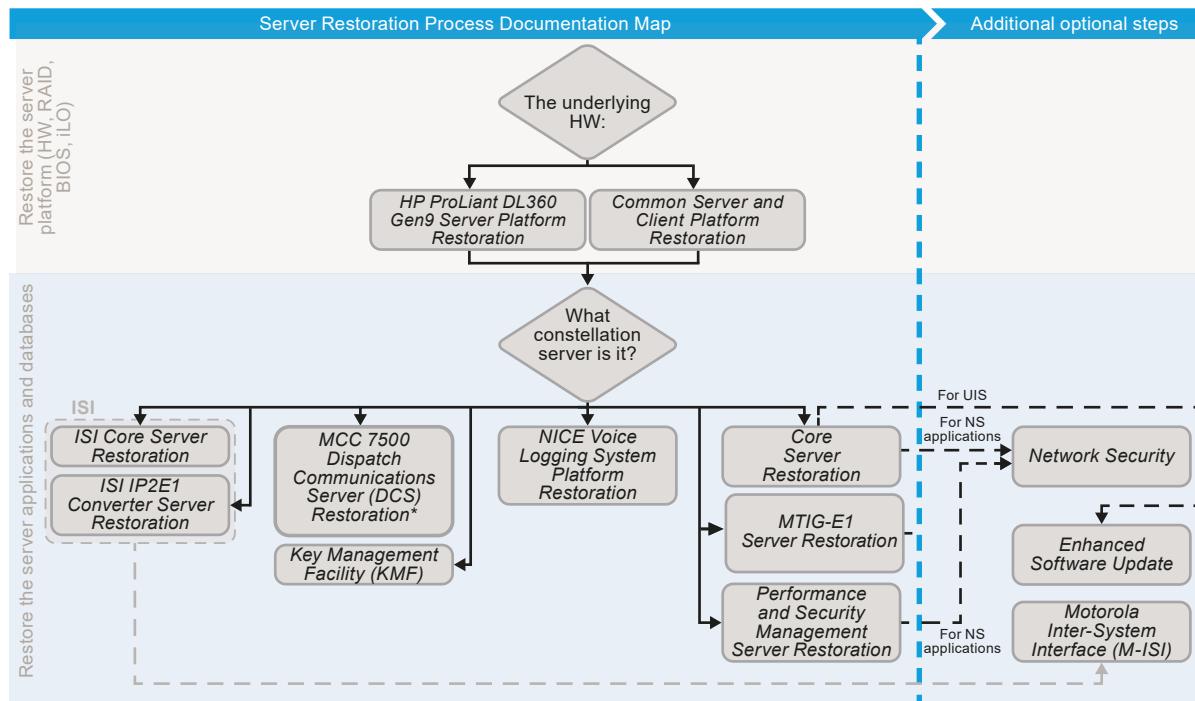
Convention	Description
Bold	This typeface is used for names of, for instance, windows, buttons, and labels when these names appear on the screen (example: the Alarms Browser window). When it is clear that we are referring to, for instance, a button, the name is used alone (example: Click OK).
Monospacing font	This typeface is used for words to be typed in exactly as they are shown in the text (example: In the Username field, type Admin).
	This typeface is used for messages, prompts, and other text displayed on the computer screen (example: A new trap destination has been added).
<i><Monospacing font in bold Italic></i>	This typeface is used with angle brackets as placeholders for a specific member of the group that the words represent (example: <i><router number></i>).  NOTE: In sequences to be typed in, the angle brackets are omitted to avoid confusion whether to include the angle brackets in the text to be typed.
CAPITAL LETTERS	This typeface is used for keyboard keys (example: Press Y and press ENTER).
<i>Italic</i>	This typeface is used for citations. A citation usually is the name of a document or a phrase from another document (example: <i>DIMETRA System Overview</i>).
→	An → (arrow pointing right) is used for indicating the menu or tab structure in instructions on how to select a certain menu item (example: File → Save) or a certain sub-tab.

Chapter 1

Server Software Restoration

Figure 1: Server Restoration Process Documentation Map

This figure presents the relation between manuals describing how to restore a server in a DIMETRA system.



*For standalone MCC 7500 Dispatch Communications Servers.

NOTE: This manual describes only the process of restoring one of the application servers running on the Core Server. If you want to restore the Core Server hardware, see the *Common Server and Client Platform Restoration* manual or the *HP ProLiant DL360 Gen9 Server Platform Restoration* manual.

Before you begin any restoration activities, ensure the server platform is configured properly. For details on the technical specification and hardware setup, see the *Common Server and Client Platform Restoration* manual or the *HP ProLiant DL360 Gen9 Server Platform Restoration* manual.

1.1

Server Restoration Prerequisites

Before restoring a server, ensure that you have the required software, passwords, licenses, and other necessary items enlisted in the table below.

IMPORTANT: Check for any new Motorola Solutions Technical Notifications (MTNs) before starting the restoration procedures.

Table 1: Core Server Restoration Prerequisites

Type	Description
Software	Combined DVD 1 – HPE Server Gen9 and Gen10

Type	Description
	<i>Combined DVD III</i>
	<i>Combined DVD V</i>
	<i>Authentication Centre DVD</i>
	<i>Combined DVD II</i>
	<i>System Accounts CD</i>
	<i>System Keys CD</i>
	<i>FlexCD containing the customized IP plan (if required)</i>
	<i>Network Security DVD DISK1</i>
	<i>Network Security DVD DISK2</i>
	<i>TLS DVD</i>
	<i>DCS DVD</i>
	<i>Red Hat Patch DVD (optional)</i>
	<i>RHEL Motopatch DVD (optional)</i>
Other	Password list
	iLO license
	iLO interface IP address
	iLO credentials: user name and password
	System Accounts ID
	System Keys ID



NOTE: The installation media can be obtained from the **Motorola Solutions Security Update Service**:
<https://sites.google.com/a/motorolasolutions.com/sus-motopatch>.



NOTE: When installing or reinstalling the application server from the Combined DVDs, use a bundle of DVDs appropriate for the used version of the Combined DVD. Do not mix DVDs from different bundles, unless you are informed to do so.

1.2

Obtaining the License Manager UUID

The License Manager UUID is one of the items necessary for completing the restoration process of the application servers running on the Core Server.

Procedure:

1. Go to <http://licensing.motorolasolutions.com>. The logon dialog window appears.
2. Perform one of the following actions:

If...	Then...
If you are not a new website user,	<ol style="list-style-type: none"> a. Enter the user name and password. b. Click Login.

If...	Then...
If you are a new website user,	<ol style="list-style-type: none"> Click New User? Enter the credentials required to register. Click Complete.

You are logged on to the **Motorola Solutions Self-Service Licensing Portal**.

- Search for the entitlement ID using the Order Information from the Software License Entitlement email.
- In the **Devices Activated** section, obtain the UUID by locating and copying the Device ID number written in blue.

1.3

Restoring Primary/Secondary Core Server Applications

Prerequisites: Connect the network interface card of the server.

Obtain the License Manager UUID. See [Obtaining the License Manager UUID on page 38](#).

Check the iLO (integrated Lights Out) license status. See [Checking iLO License Status on page 63](#).

Procedure:

- Connect directly to the server by using a KVM or a monitor and keyboard.
- Perform one of the following actions:
 - If the server is not on, apply power to the server and insert the *Combined DVD I – HPE Server Gen9 and Gen10* disk.
 - If the server is on, reboot it and insert the *Combined DVD I – HPE Server Gen9 and Gen10* disk.
- On the **HP ProLiant** start-up screen, enter the **Boot Menu** by pressing F11.
- From the list, select **CD/DVD**, and press ENTER.

The server boots from the installation DVD.



NOTE: The KVM Hypervisor boot may take a couple of minutes.

- Select **Install – via vga (tty0)** and press ENTER.

After the installation finishes, the following prompt appears:

Do you want to continue the installation (y,n) [y]?

- Enter: y

The list of available cluster types appears.

1. Dimetra Core Cluster 2. Dimetra ISI Cluster Enter Cluster type (1-2) :

- Enter: 1 for the DIMETRA Core Cluster.

The list of available constellations appears:

1. Primary Core Server 2. Secondary Core Server 3. Dispatch Communication Server
4. Secure Dispatch Communication Server 5. Primary Standalone AUC 6. Secondary
Standalone AUC 7. MTIG-E101 8. MTIG-E102 Enter constellation (1-8) :

8. Enter the number for **Primary Core Server** or the **Secondary Core Server**.

The following message appears:

Do you want to install with Customized IP Plan (y, n) [n]?

9. Perform one of the following actions:

If...	Then...
If you want to use the default IP plan,	<p>perform the following actions:</p> <ul style="list-style-type: none"> a. Enter: n b. Enter the Zone ID (1-56). c. Enter the Cluster ID (1-16).
If you want to use the customized IP Plan,	<p>perform the following actions:</p> <ul style="list-style-type: none"> a. Enter: y b. Enter the Zone ID (1-56). c. Enter the Zone Octet (1-127). d. Enter the Cluster ID (1-16). e. Enter the Cluster Octet (1-127).

10. Enter the lowest zone octet number in the local cluster and in the local MSO.

11. When asked about the Geographic and Local Redundancy configuration, enter: no

The following message appears:

Enter Encrypted Call Logging Status: 0=Off, 1=On [0]?

12. Enter: 0 or 1

The following message appears:

Please select AUC role:

1. Active
2. Standby

13. At the prompt, enter the number reflecting the AUC role in the system.

The following message appears:

Shall Enhanced Auc be configured with PrC functionality disabled (y, n) [n]?

14. Enter: y or n

15. At the prompt, enter the System Accounts ID using numerals and capital letters (five characters).

16. Enter the System Keys ID (SSHCD ID).

The following message appears:

Forward the System Logs (Syslogs) to Centralized Event Logging server? (y, n) [n]?

17. Enter: y or n

If you chose to forward the logs to the Centralized Event Logging Server, the following messages appear:

Please enter the primary syslog server address:

Please enter the second syslog server address:

18. Enter the addresses of the syslog servers.

The following message appears:

Install AV Protection on All Application Servers? (y,n) [n]?

19. Enter y or n

If you chose to install AV Protection, the following message appears:

Enter the Zone Octet for AV Server that manages AV Clients in this Zone (1-127):

20. Enter the appropriate value.

The following message appears:

Do you have subscription for Security Update Service (y,n) [n]?



IMPORTANT: Ensure that you have RHEL Motopatch and RHEL 7 Media disks.

21. Enter: y or n

The following message appears:

If you have License Manager UUID for your server, please enter it now, or just press ENTER to skip installing License Manager UUID (you can install it later)
Please enter the License Manager UUID in the following format: XXXXXXXX-XXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX (spaces and other separators - . : will be ignored and UUID will be reformatted)

22. Enter the License Manager UUID obtained from the License Inquiry Tool.

The following message appears:

Please confirm the UUID is correct (y,n) [n]?

23. Verify that the UUID is correct and enter y

24. Enter the number for your time zone.

A list of time zones and the following message appear:

Press <ENTER> to list more timezones or enter number to choose timezone

25. Enter the number for your time zone. To list more time zones than initially displayed, press ENTER.

A prompt with installation details and the following message appear:

Confirm the configuration settings are correct (y,n) [y]?

26. If the installation settings are correct, enter: y



NOTE: If you enter n, the installation process goes back to [step 6](#).

The following message appears:

Do you want to proceed with the server installation (y,n) [y]?

27. Start the installation process by entering: y



NOTE:

If you enter n, the following message appears:

```
!!!!!!!!!!!!!! WARNING !! WARNING !! WARNING !!!!!!! Aborting the
installation will not install the new software. Do you want to proceed with
the server installation (y,n) [y]?
```

Entering n reboots the system.

The installation process starts and the server reboots automatically.

28. Follow on-screen instructions and, at the prompt, insert an appropriate installation disk.

The disk sequence depends on your system configuration and the options you selected in the initial part of the installation process. The full installation process may take up to several hours.

Postrequisites: Change the ilouser and Administrator passwords. See [Changing the iLO User Password on page 74](#).



NOTE: Changing the passwords is recommended for security reasons.

1.4

Service Redundancy Solution

Service Redundancy Solution (SRS) enables automatic switch-over between redundant devices. When SRS is in automatic mode, the secondary device remains in the standby mode and its common data is synchronized with the active device. If the active device fails, the standby device automatically takes over the service.

SRS is available for selected devices only, currently it is used with:

- Short Data Routers (SDR)
- Packet Data Gateway (PDG)
- Air Traffic Router (ATR)
- MultiCADI
- Alias Server

The SRS should be used in automatic mode, but using UEM, the administrator can manually configure redundancy state of the devices. Manual setup can be used when the operator wants to control which device delivers the service. For information on viewing the redundancy information of a device, see the *Unified Event Manager* manual.

1.4.1

Viewing Redundancy Information of a Device

Procedure:

1. In the **Network Database** window, right-click the desired device.
2. From the drop-down menu, select **Redundancy** → **Show**.

For Alias Server, you must first perform site/network discovery for each of the zones. See [Discovering Groups of Devices on page 44](#).



NOTE:

In the **Discovery Type** drop-down list, you must select **Application Servers**.

Ensure that the generic node or nodes are also discovered.

Result: The **Redundancy State** window appears, showing information on the redundancy state of the device.

1.4.2

Changing Redundancy State of a Device

Prerequisites:

Perform the following actions:

- Verify that two redundant devices are installed in the zone.
- For Alias Server, perform site/network discovery for each of the zones. For information on discovering devices, see the *Unified Event Manager* manual.



NOTE:

In the **Discovery Type** drop-down list, you must select **Application Servers**.

Ensure that the generic node or nodes are also discovered.

Procedure:

1. In the **Network Database** window, right-click the device of your choice.
 - Short Data Router
 - Packet Data Gateway
 - Air Traffic Router
 - Alias Server
 - MultiCADI
2. From the drop-down menu, select **Redundancy** → **Actions**.
3. From the upper drop-down list, select the ID of the device that you want to configure.
4. From the **Action** drop-down list, select the desired action and click **Apply**.
5. Confirm the change in the pop-up windows.

1.4.3

Discovering Groups of Devices

Discovering a group of devices is sometimes referred to as subnet discovery. You can manually discover groups of devices that perform a joint function or serve one purpose, for example a Mobile Switching Office (MSO), or a Console Site.

 **IMPORTANT:** Subnet discovery does not discover the MTIG-E1 hardware agent. If you use MTIG-E1, you have to discover its hardware agent as a single device (node discovery) by using the Generic Application Server (GAS) IP address of MTIG-E1.

 **NOTE:** UEM attempts to discover all IP addresses for a selected network type that are defined in the IP plan. However, some IP addresses (devices) may not be present in the network. Check discovery logs by clicking **Discovery Job** in the **Job Status View** dialog box. The discovery logs contain details of the IP addresses that are discovered and IP addresses that are not reachable. Confirm that devices that are not reachable are not configured in the network. For more details, check the network plan or execute an ICMP ping on the unreachable IP addresses.

Procedure:

1. In the **Navigation View** panel, click the **Network Database** node.
2. From the main menu, select **Tools** → **Discovery Configuration**.
3. In the **Discovery Configuration** window, from the **Discovery Type** drop-down list, select a network type.
4. Optional: Type the site identifier. Click **Start Discovery**.
5. In the **View Job Status** window, click **View Job Status**.

 **NOTE:** UEM constructs the range of IP addresses for the selected discovery type. This operation depends on the system IP and the site identifier, if any, that you provide. UEM attempts to discover all IP addresses in the subnet, even though some IP addresses (devices) may not exist in the network.

Result: The **Job Status View** dialog box appears, displaying the status of the subnet discovery.

1.4.4

Discovery Status

The status of a discovery job is displayed in the **Job Status View** window. Status messages include:

In progress

The job submission has been recognized and is in the queue. To determine if the job has started executing and to get information on the progress, view the job log.

Success

The discovery job has completed successfully. One or more devices may still have not been found due to communication failures. This information is shown in the field and detailed information is available in the job log.

Failure

The discovery job has failed. The job has terminated abnormally. The job log provides additional details and it is necessary for the user to re-submit the job at a later time.

After the job is complete, select the job and click **View Log**. Confirm that IP addresses that are not reachable are indeed not configured in the network. Check the network plan or, by executing an Internet Control Message Protocol (ICMP), ping on the unreachable IP addresses.

1.4.5

Redundancy State Window

Table 2: Parameters for the Redundancy State Window

Name	Description
<ul style="list-style-type: none"> • Short Data Router • Packet Data Gateway • Air Traffic Router • MultiCADI • Alias Server 	The ID of the device.
SDR/PDG/ATR/MultiCADI/AS Operation Mode	The current operation mode (fault state) of the device, value depends on implementation.
Redundancy Service Mode	<p>The current redundancy state of the device:</p> <ul style="list-style-type: none"> • ACTIVE • STANDBY • MAINTENANCE • FORCE ACTIVE • FORCE STANDBY • FORCE MAINTENANCE
Redundancy Service Reason	The reason for the current redundancy state.
Synchronization State	<p>Current synchronization state of the device:</p> <ul style="list-style-type: none"> • SYNCHRONIZED • SYNCHRONIZING • UNSYNCHRONIZED
Synchronization Reason	<p>Cause of current synchronization state:</p> <ul style="list-style-type: none"> • NORMAL • INITIALIZING • INVALID CONFIGURATION • LINK DOWN • VERSION MISMATCH • SYNCHRONIZATION ERROR • APPLICATION DISABLED
Additional Info	Additional Information reported by the device.
Last Synchronized	Date and time of the last synchronization.

1.5

Logging On to iGAS Through a Terminal Server

Prerequisites:

Power on the server.

Procedure:

1. Start PuTTY.
2. Optional: In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.



NOTE: Newer versions of PuTTY (such as version 0.70) do not require this step.

3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter the applicable terminal server address:
 - For Primary/Location A MSO Terminal Server: 10.<Z0>.233.222
 - For Secondary/ Location B MSO Terminal Server: 10.<Z0>.233.223
 - For Console/DCS Site Terminal Server: 10.<Z0>.SITE.51
 - For BTS/Wave sites: 10.<Z0+127>.SITE.51

where <Z0> is the zone octet where the terminal server is located.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: motorola
8. At the prompt, enter the password.
9. Enter the number for the server to which you want to log on.
10. At the logon prompt, enter the user logon name.
11. At the password prompt, enter the current password.

The iGAS start-up screen appears.

1.5.1

Messages Appearing when Establishing a Secure Session

When establishing a secure session with iGAS or an application server, messages appear indicating different server states and possible risks.

The following table contains example messages likely to appear when logging on to a server.



NOTE: The IP addresses and RSA key fingerprints are unique per server and vary depending on the system configuration.

Table 3: Messages Appearing when Establishing a Secure Session

Message Example	Explanation
<p>If you want to carry on connecting but without updating the cache, hit No. If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.</p> <p>where</p> <p><yyyy:yyyy:yyyy:yyyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy> are RSA key fingerprints of the server.</p>	<p>tem, it is an indication of a potential security breach.</p> <p>WARNING: Regardless of the possible cause for displaying the messages, notify the system administrator about a potential security breach.</p>

1.6

Logging On to iGAS Through a KVM Switch

Before performing any operations in the iGAS menu of a server, connect directly to the server by using a Keyboard Video Mouse (KVM) switch or a monitor and a keyboard, and log on with one of the user accounts.

Prerequisites: Power on the server.

Procedure:

1. Connect directly to the server by using a KVM switch or a monitor and a keyboard.
2. At the logon prompt, enter the user logon.
3. At the password prompt, enter the password.

The main menu for the selected user appears.

1.7

Checking the Installation Log

Accessing the installation log allows you to verify if it contains any unresolved errors.

Prerequisites: Log on to iGAS as `instadm` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **View Installation Log**.

The installation log status message appears.

3. Press **SPACE** several times to continue to the end of the message.

4. View the status information to verify that it does not contain unresolved errors.

1.8

Checking RAID Configuration Status

Checking the RAID configuration status allows you to verify if the configuration is successfully completed.

Procedure:

1. Log on to integrated Lights Out (iLO) with the ilouser user role.
2. From the left-hand menu, select **Information** → **System Information**.
3. Select the **Storage** tab.
4. In the **Storage Information** section, perform the following actions:
 - a. Select the **Logical View** radio button and verify if the **Controller Status** is **OK**.
 - b. Verify if the **Cache Module Status** is **OK**.
 - c. Verify if **Fault Tolerance** is set to:
 - RAID 1, if two hard drives were installed
 - RAID 1+0, if four or eight hard drives were installed
 - d. Select the **Physical View** radio button and verify if the **Controller Status** is **OK**.
 - e. Check if **Cache Module Status** is **OK**.

The list of drives with their individual statuses are available under both **Logical View** and **Physical View**.

1.9

Displaying iGAS Version and Server Information

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At the logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

```
Unix Administration -----
1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Enter the number for **Display IGAS version**.
4. Enter the number for **Display server information**.

Hostname appears in one of the following formats: `z <XXX>igas-prim-cs` or `z <XXX>igas-sec-cs` where `<XXX>` is the zone ID.

The IP Address is in the following format:

- For primary Core Server/ISI Core Server: `10. <Z0+127>114.108/24`
- For secondary Core Server/ISI Core Server: `10. <Z0+127>114.110/24`

Examples: `10.137.114.108/24` or `10.137.114.110/24`

A message similar to the following appears:

```
Hostname is : z010igas-prim-cs Domain is : zone10 Hostid is : f0231918 MAC Address
is : 00:0c:29:3c:64:8d IP Address is : 10.137.114.108/24 : Active Boot Environment
free space : 6.4G Filesystem 'storage' free space : 16G Filesystem 'datastore1'
free space : 463.9G System installed on : HDD Uptime information : 1 days, 4
hour(s) System Accounts ID : XXXXXX License Manager UUID : AAAAAAAA-BBBB-CCCC-DDDD-
EEEEEEEEEE
```

1.10

Rebooting the Physical Server

Prerequisites: Log on as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Unix Administration**.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Reboot the physical server by entering the number associated with **Reboot physical server**.

1.11

Configuring Time Synchronization

Process:

Depending on the server to be configured, see one of the following scenarios:

Table 4: Primary/Secondary Core Server – Time Synchronization

Server type	NTS present	Zone	Procedure to perform
Primary Core Server	Yes	Lowest Zone Octet, Lowest Cluster Octet	<p>a. Configuring Initial Time Service – Primary Core Server in the Lowest Zone Octet, Lowest Cluster Octet on page 56</p> <p>b. Forcing Time Synchronization to the NTP Server on page 61</p>
		Other	<p>a. Configuring Initial Time Service – Other Primary Core Servers on page 58</p> <p>b. Forcing Time Synchronization to the NTP Server on page 61</p>
No		Lowest Zone Octet, Lowest Cluster Octet	<p>a. Disabling Local Clock Monitor on Secondary Core Server on page 52</p> <p>b. Synchronizing with Secondary Core Server on page 53</p> <p>c. Enabling Local Clock Monitor on Secondary Core Server on page 55</p> <p>d. Configuring Initial Time Service – Primary Core Server in the Lowest Zone Octet, Lowest Cluster Octet on page 56</p>
		Other	<p>a. Configuring Initial Time Service – Other Primary Core Servers on page 58</p> <p>b. Forcing Time Synchronization to the NTP Server on page 61</p>

Server type	NTS present	Zone	Procedure to perform
Secondary Core Server	N/A	N/A	<ul style="list-style-type: none"> a. Configuring Initial Time Service – Secondary Core Server on page 59 b. Forcing Time Synchronization to the NTP Server on page 61

1.11.1

Disabling Local Clock Monitor on Secondary Core Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

System Administrator Main Menu

1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management

Please enter selection (1-8, q) [q]:

2. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Enter the number for **NTP Administration**.

The **NTP Administration** menu appears.

```
NTP Administration ----- 1. Enable NTP service 2. Disable NTP
service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
parameters 6. Change date and time Please enter selection (1-6, q) [q]:
```

4. Enter the number for **Change NTP servers parameters**.

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,
q) [q]:
```

5. Enter the number for **Manage local clock**.

The **NTP server: Local server** menu appears:

```
NTP server: Local ----- 1. Add server to list 2. Remove server from list 3. Show if server is on the list 4. Show server configuration 5. Update server configuration 6. Sync down iGAS time to local hypervisor. 7. Manage Local Clock Monitor Please enter selection (1-7, q) [q]:
```

6. Enter the number for **Manage Local Clock Monitor**.

The **Manage Local Clock Monitor** menu appears:

```
Manage Local Clock Monitor ----- 1. Enable LCM 2. Disable LCM 3. Show LCM configuration and status 4. Update LCM configuration Please enter selection (1-4, q) [q]:
```

7. Enter the number for **Disable LCM**.

One of the following message appear:

```
LCM was successfully disabled.
```

or

```
LCM is already disabled.
```

8. In the command line, enter: q

9. Keep pressing ENTER until the **NTP server: Local** menu appears.

10. Enter the number for **Add server to list**.

One of the following messages appears:

```
Updated NTPD configuration was activated. NTP server was added to list.
```

or

```
NTP server 127.127.1.0 already added to list.
```

1.11.2

Synchronizing with Secondary Core Server

Perform this procedure for the Primary Core Servers in the Lowest Zone Octet, Lowest Cluster, without physical NTS.

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Enter the number for **NTP Administration**.

The **NTP Administration** menu appears.

```
NTP Administration ----- 1. Enable NTP service 2. Disable NTP
service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
parameters 6. Change date and time Please enter selection (1-6, q) [q]:
```

4. Enter the number for **Change NTP servers parameters**.

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,
q) [q]:
```

5. Enter the number for **Manage tertiary NTP server**.

The **Tertiary NTP server** menu appears.

```
NTP server: Tertiary ----- 1. Add server to list 2. Remove server
from list 3. Show if server is on the list 4. Show server configuration 5. Update
server configuration 6. Sync down time to this server Please enter selection (1-6,
q) [q]:
```

6. Verify that the synchronization to the server is not allowed by entering the number for **Show server configuration**.

The server information messages appear.

```
Server IP address: <IP address> Synchronization to server is not allowed Option
'true' is not set Option 'burst' is not set Option 'iburst' is not set Option
'minpoll' is set and its value is 6 (1 min) Option 'maxpoll' is set and its value is
10 (17 min)
```

7. In the **NTP server** menu, enter the number for **Update server configuration**.

The following message appears:

```
Provide NTP server IP (IP_addr, q) [<IP address>]:
```

8. Set the server address to be the address of the Secondary Core Server in the same zone by entering:
10.<Z0>.233.12

A number of additional configuration questions appear.

9. Leave the default values for all the configuration settings.



NOTE:

The default values are the ones in square brackets, for example:

```
[n]
```

The **NTP server menu** appears.

10. Keeping entering: q until you get back to the **NTP servers administration** menu.

11. In the **NTP servers administration** menu, enter the number for **Manage tertiary NTP server**.

The **NTP server** menu appears.

```
NTP server: Tertiary ----- 1. Add server to list 2. Remove server
from list 3. Show if server is on the list 4. Show server configuration 5. Update
```

```
server configuration 6. Sync down time to this server Please enter selection (1-6,  
q) [q] :
```

12. Enter the number for Sync down time to this server.

The following messages appear:

```
WARNING !!! Be careful using this option. Forcing Time Sync Down can cause time  
jumps, what can be dangerous for running applications. Forcing Time Sync Down can  
cause NTPD daemon to panic on this or on remote server. On successful Time Sync  
Down, CMA agent will be restarted on the host, which can cause interim UEM alarms  
for iGAS and hypervisor of the host. Please ignore them. WARNING !!!Do you really  
wish to continue? (y,n,q) [n] :
```

13. Enter: y

The message about the successful time synchronization similar to the following one appears.

```
Synchronizing time on hypervisor to 10.20.233.88 Synchronizing time on iGAS to  
10.20.233.88 Restarting CMA agent, please ignore interim UEM alarms for this iGAS.  
and hypervisor Restart completed Time Sync Down successfully executed on iGAS.  
Time correction +0.000209 s. Time Sync Down successfully executed on hypervisor.  
Time correction +0.001438 s. Running Local Clock Monitor in the background to  
update local clock driver
```

14. Keep entering: q until you get back to the NTP Administration menu.

15. Enter the number for Enable NTP service.

The **NTP Administration** menu appears.

16. If the time correction on iGAS was greater than 1 minute, repeat this procedure.

Postrequisites:

 **CAUTION:** Before proceeding to the next procedure, ensure that the synchronization was successful.
Otherwise, you risk damaging the system.

1.11.3

Enabling Local Clock Monitor on Secondary Core Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu appears:**

```
System Administrator Main Menu  
-----  
1. Enable all Application Servers  
2. Disable all Application Servers  
3. Display Status of all Application Servers  
4. Unix Administration  
5. Application Servers Administration Menus  
6. Application Servers Boot/Reboot/Shutdown  
7. Application Servers Status Administration  
8. Application Isolation Management  
Please enter selection (1-8, q) [q] :
```

2. Enter the number for Unix Administration.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Enter the number for **NTP Administration**.

The **NTP Administration** menu appears.

```
NTP Administration ----- 1. Enable NTP service 2. Disable NTP
service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
parameters 6. Change date and time Please enter selection (1-6, q) [q]:
```

4. Enter the number for **Change NTP servers parameters**.

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,
q) [q]:
```

5. Enter the number for **Manage local clock**.

The **NTP server: Local** menu appears:

```
NTP server: Local ----- 1. Add server to list 2. Remove server from
list 3. Show if server is on the list 4. Show server configuration 5. Update
server configuration 6. Sync down iGAS time to local hypervisor. 7. Manage Local
Clock Monitor Please enter selection (1-7, q) [q]:
```

6. Enter the number for **Manage Local Clock Monitor**.

The **Manage Local Clock Monitor** menu appears:

```
Manage Local Clock Monitor ----- 1. Enable LCM 2. Disable
LCM 3. Show LCM configuration and status 4. Update LCM configuration Please enter
selection (1-4, q) [q]:
```

7. Enter the number for **Enable LCM**.

The following message appears:

```
LCM was successfully enabled.
```

1.11.4

Configuring Initial Time Service – Primary Core Server in the Lowest Zone Octet, Lowest Cluster Octet

 **NOTE:** Perform this procedure for the Primary Core Server in the Lowest Zone Octet belonging to the cluster with the lowest octet.

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
```

```
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for Unix Administration.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Enter the number for NTP Administration.

The **NTP Administration** menu appears.

```
NTP Administration ----- 1. Enable NTP service 2. Disable NTP
service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
parameters 6. Change date and time Please enter selection (1-6, q) [q]:
```

4. Enter the number for Display NTP status.

5. If the NTP service is not started, in the **NTP Administration menu, perform the following actions:**

- Enter the number for **Disable NTP service**.
- Enter the number for **Enable NTP service**.
- After a several minutes, verify that the NTP is started by entering the number for **Display NTP status**.



NOTE: For correct operation, NTP requires proper BIOS setup (date and time).

6. Enter the number for Change NTP servers parameters.



NOTE: The NTP service has to be started. If not, go to [step 5](#).

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,
q) [q]:
```

7. Enter the number for Set initial NTP servers configuration.

The following message appears:

```
Warning! Calling this option will reset current NTP settings. Do you wish to
continue (y,n,q) [n]:
```

8. Enter: y

The following message appears:

```
What is the lowest Cluster Octet in system? (1-127, q) [q]:
```

9. Enter the lowest cluster octet number.

The following message appears (only if the lowest cluster octet in the system is the same as the cluster octet of the server you are configuring):

What is the lowest zone octet in the next MSO? Press ENTER if not available
(1-127, q) [0]:

10. Enter the number of the Lowest Zone Octet in the next MSO.

 **NOTE:** In a system within multiple MSOs, the term *next MSO* refers to the other MSO location that preferably deploys a Network Time Server.

The following message appears:

Updated NTPD configuration was activated. NTP initial configuration was successfully created. LCM was successfully updated.

1.11.5

Configuring Initial Time Service – Other Primary Core Servers

 **NOTE:** Perform this procedure for the Primary Core Server in the Lowest Zone Octet belonging to the cluster with the lowest octet.

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

System Administrator Main Menu

1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:

2. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

Unix Administration ----- 1. Reboot physical server 2. Shutdown physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6. Display IGAS version 7. Display server information Please enter selection (1-8, q) [q]:

3. Enter the number for **NTP Administration**.

The **NTP Administration** menu appears.

NTP Administration ----- 1. Enable NTP service 2. Disable NTP service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers parameters 6. Change date and time Please enter selection (1-6, q) [q]:

4. Enter the number associated with the **Display NTP status** option.

5. If the NTP service is not started, in the **NTP Administration** menu, perform the following actions:

a. Enter the number for **Disable NTP service**.

- b. Enter the number for **Enable NTP service**.
- c. After a several minutes, verify that the NTP is started by entering the number for **Display NTP status**.



NOTE: For correct operation, NTP requires proper BIOS setup (date and time).

6. Enter the number for **Change NTP servers parameters**.



NOTE: The NTP service has to be started. If not, go to [step 5](#).

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,
q) [q] :
```

7. Enter the number for **Set initial NTP servers configuration**.

The following message appears:

```
Warning! Calling this option will reset current NTP settings. Do you wish to
continue (y,n,q) [n] :
```

8. Enter: y

The following message appears:

```
What is the lowest Cluster Octet in system? (1-127, q) [q] :
```

9. Enter the lowest cluster octet number.

The following message appears:

```
Updated NTPD configuration was activated. NTP initial configuration was
successfully created. LCM was successfully updated.
```

The initial NTP configuration has been completed.

1.11.6

Configuring Initial Time Service – Secondary Core Server



NOTE: Perform this procedure on the Secondary Core Server.

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
```

```
8. Application Isolation Management  
Please enter selection (1-8, q) [q]:
```

2. Enter the number for Unix Administration.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown  
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.  
Display IGAS version 7. Display server information Please enter selection (1-8, q)  
[q]:
```

3. Enter the number for NTP Administration.

The **NTP Administration** menu appears.

```
NTP Administration ----- 1. Enable NTP service 2. Disable NTP  
service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers  
parameters 6. Change date and time Please enter selection (1-6, q) [q]:
```

4. Enter the number for Display NTP status.

5. If the NTP service is not started, in the NTP Administration menu, perform the following actions:

a. Enter the number for Disable NTP service.

b. Enter the number for Enable NTP service.

c. After a several minutes, verify that the NTP is started by entering the number for Display NTP status.



NOTE: For correct operation, NTP requires proper BIOS setup (date and time).

6. Enter the number for Change NTP servers parameters.

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers  
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage  
secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,  
q) [q]:
```

7. Enter the number for Set initial NTP servers configuration.

The following message appears:

```
Warning! Calling this option will reset current NTP settings. Do you wish to  
continue (y,n,q) [n]:
```

8. Enter: y

The following message appears:

```
What is the lowest Cluster Octet in system? (1-127, q) [q]:
```

9. Enter the lowest cluster octet number.

The following message appears:

```
Updated NTPD configuration was activated. NTP initial configuration was  
successfully created. LCM was successfully updated.
```

The initial NTP configuration has been completed.

1.11.7

Forcing Time Synchronization to the NTP Server

Perform this procedure for:

- Primary Core Servers



IMPORTANT: The procedure should be performed on the Primary Core Server **unless** it is located in the Lowest Zone Octet, Lowest Cluster Octet, and there is no NTS in either local MSO or the next MSO. In this case, see [Configuring Time Synchronization on page 51](#).

- Secondary Core Servers

Prerequisites:

For the Primary Core Server, ensure that you configured the initial time service. See:

- [Configuring Initial Time Service – Primary Core Server in the Lowest Zone Octet, Lowest Cluster Octet on page 56](#)
- [Configuring Initial Time Service – Secondary Core Server on page 59](#)

For more details, see [Configuring Time Synchronization on page 51](#).

Log on to iGAS as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

```
Unix Administration ----- 1. Reboot physical server 2. Shutdown
physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
Display IGAS version 7. Display server information Please enter selection (1-8, q)
[q]:
```

3. Enter the number for **NTP Administration**.

The **NTP Administration** menu appears:

```
NTP Administration ----- 1. Enable NTP service 2. Disable NTP
service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
parameters 6. Change date and time Please enter selection (1-6, q) [q]:
```

4. Enter the number for **Change NTP servers parameters**.

The **NTP servers administration** menu appears.

```
NTP servers administration ----- 1. Set initial NTP servers
configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
```

secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5, q) [q] :

5. Enter the number for one of the following options:

Table 5: NTP Servers Administration Menu – Settings

Server type	Zone	NTS in local MSO	NTS in next MSO	Option to choose
Primary Core Server	Lowest Zone Octet, Lowest Cluster Octet	Yes	N/A	Manage primary NTP server
		No	Yes	Manage secondary NTP server
		No	No	Do not perform this procedure.
	Other	Yes	N/A	Manage primary NTP server
		No	N/A	Manage secondary NTP server
Secondary Core Server	N/A	Yes	N/A	Manage primary NTP server
		No	N/A	Manage secondary NTP server

The NTP server menu appears. The following example applies to the secondary server.

NTP server: Secondary ----- 1. Add server to list 2. Remove server from list 3. Show if server is on the list 4. Show server configuration 5. Update server configuration 6. Sync down time to this server Please enter selection (1-6, q) [q] :

6. Enter the number for **Sync down time to this server**.

A number of messages appear concluded with the following prompt:

Do you really wish to continue? (y, n, q) [n] :

7. Enter: y

A message informing about the successful time synchronization appears.

Restarting CMA agent, please ignore interim UEM alarms for this iGAS and hypervisor. Restart completed. Time Sync Down successfully executed on iGAS. Time correction +0.010284 s. Time Sync Down successfully executed on hypervisor. Time correction -0.003540 s.

 **NOTE:** Upon successful time synchronization, CMA agent on iGAS restarts and transient alarms on UEM for synchronized host may appear. You should ignore them.

8. Keep entering: q until you get back to the **NTP Administration** menu.

9. Enter the number for **Enable NTP service**.

The message about enabled NTP service appears.

Hypervisor: NTP service is already enabled. iGAS: NTP service is already enabled.

10. After at least 20 minutes, verify if the synchronization occurred by performing the following actions:

- a. Get back to the **NTP Administration** menu.
- b. Enter the number for **Display NTP status**.

1.12

Configuring iLO Security

Procedure:

1. Log on to iLO with the **Administrator** user role.

If...	Then...
If you want to configure iLO 4 security,	perform the following actions: <ol style="list-style-type: none">In the left-hand side panel, select Administration → Security.Select the Encryption tab.In the Encryption Enforcement Settings area, set the Enforce AES/3DES Encryption option to Enabled.
If you want to configure iLO 5 security,	perform the following actions: <ol style="list-style-type: none">In the left-hand side panel, click Security.Select the Encryption tab.In the Security Settings area, set the Production option.

2. Click **Apply**.

Result: The browser connection ends and the iLO interface restarts.

1.13

iLO Configuration Verification

1.13.1

Checking iLO License Status

Procedure:

1. Log on to integrated Lights Out (iLO) as an Administrator.
2. From the left-hand side menu, select **Administration**.
3. Click the **Licensing** tab.

The Current License Status appears.

 **NOTE:** If there is no current iLO license installed, see "Installing the iLO License" in *Common Server and Client Platform Restoration*.

1.14

License Manager Post-Restoration Operations

If you are replacing a server component, replacing hardware, or performing the software restoration only, restore the License Manager from backup.

Prerequisites: If you are performing License Manager database restoration, boot and configure Upgrade Install Server (UIS). See [Booting Primary/Secondary Core Server Application Servers on page 66](#) and UIS configuration procedures in [UIS – Software Application Restoration on page 93](#).

Process:

1. Boot the License Manager only. For details, see [Booting Primary/Secondary Core Server Application Servers on page 66](#).
2. Depending on the restoration scenario, perform one of the following actions:
 - Restore the License Manager database. For details, see [License Manager – Software Application Restoration on page 211](#). After that, enable the License Manager using [Enabling the Application Server on page 66](#).
 - Enable the License Manager using [Enabling the Application Server on page 66](#). Then, upload the license files to the system. See [Uploading Licenses to the License Manager on page 67](#).
3. Boot the remaining application servers. See [Booting Primary/Secondary Core Server Application Servers on page 66](#).

1.14.1

Verifying the License Manager UUID

Prerequisites: Log on as `instadm` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **License Administration**.

The **License Administration** menu appears.

```
License Administration ----- 1. Show License Manager UUID 2.
Update License Manager UUID Please enter selection 1-2, q) [q]:
```

3. Enter the number for **Show License Manager UUID**.

The **Assigned License Manager UUID** appears.

4. Verify the UUID.

Result: If the UUID is incorrect, continue to [Updating the License Manager UUID on page 65](#).

1.14.2

Updating the License Manager UUID

Prerequisites: Verify the UUID is incorrect. See [Verifying the License Manager UUID on page 64](#).

Process:

1. Shut down License Manager. See [License Manager – Disabling Application Server on page 211](#).
2. Change the UUID. See [Changing the License Manager UUID on page 65](#).
3. Reinstall the License Manager. See [License Manager – Restoring Application on page 212](#).
4. Enable the License Manager server. See [License Manager – Enabling the Application Server on page 213](#).
5. Upload The licenses. See [Uploading Licenses to the License Manager on page 67](#).

1.14.2.1

Changing the License Manager UUID

Prerequisites: Log on as `instadm` using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **License Administration**.

The **License Administration** menu appears.

```
License Administration ----- 1. Show License Manager UUID 2.
Update License Manager UUID Please enter selection 1-2, q) [q]:
```

3. Enter the number for **Update License Manager UUID**.

The following message appears:

```
Please Enter the new License Manager UUID:
```

4. Enter the new UUID.

System prompts you to confirm the License Manager UUID is correct.

5. Enter **y** to confirm.

The following message appears:

```
License Manager UUID was updated successfully. Note: Manual reinstallation of
License Manager is needed.
```

Postrequisites: Continue to [License Manager – Restoring Application on page 212](#).

1.14.3

Booting Primary/Secondary Core Server Application Servers

Prerequisites:

Before performing the application boot, ensure that relevant licenses are present in the system. Only the applications for which you have licenses can boot.

Log on to iGAS as sysadmin. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

3. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

4. Perform one of the following actions:

- If you want to boot all applications at once, enter the number associated with **Boot all applications**.
- If you want to boot a particular application, enter the number associated with that application.

1.14.4

Enabling the Application Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
```

```
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.
A message appears showing that the application server is enabled.
5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

1.14.5

Uploading Licenses to the License Manager

In the DIMETRA system, each zone has a License Manager.

To enable a zone or system level license, you need to upload the license to the appropriate License Manager. Load zone level licenses to the License Manager for the particular zone. Load system level licenses to the License Manager in the zone where the User Configuration Server (UCS) is located.

A separate file is generated for each License Manager in the system. Each License Manager has a unique Device ID. The Device ID encrypted in a license file issued for a particular License Manager must match the Device ID of the License Manager. The Device ID of the License Manager can be found in the bottom right corner of the License Manager User Interface (UI) web page.

 **NOTE:** Perform this procedure only if License Manager was reinstalled. Otherwise, the proper licenses are already loaded.

Prerequisites:

Obtain license files from the **My Software** portal: <http://licensing.motorolasolutions.com>

Ensure that:

- The License Manager is enabled.
- The license file is generated for this License Manager.
- The license file is available from the client machine.

Procedure:

1. Log on to the client machine.
2. Verify that the license file name matches that of its intended destination.
3. In a web browser on the PC, connect to `https://<hostname of License Server>`



NOTE: If UCS and ZDS are not booted yet, use the IP address instead of the host name.

The **Logon** page appears.

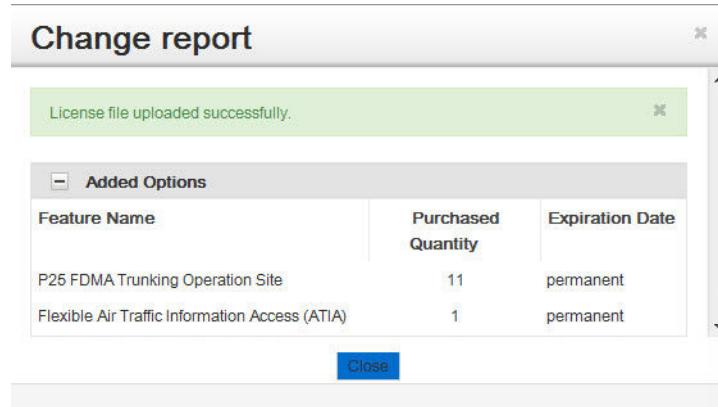
4. Log on as `lmadmin`.
5. In the top right corner of the window, click **Upload Licenses**.

If the **Upload Licenses** button is not visible in the top right corner, you may not have proper privileges.

Figure 2: Upload Licenses Button

6. In the License upload window, click **Select file**.
7. In the Choose File to Upload window, select a license file for this License Manager. Click **Open**.
8. In the License upload window, click **Upload**.

A summary of changes appears in the **Change report** window.

Figure 3: Change Report Window

9. Review the changes, and return to the License Manager UI main page by clicking **Close**.

Result: The selected license file is uploaded to the License Manager.

Postrequisites: If the User Configuration Server (UCS) was enabled during the upload of the license file to the License Manager, re-enable the UCS.

1.15

Adding Zone to a Cluster

Perform this procedure if UCS backup files are missing.

Procedure:

1. Start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.

4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter: `10.0.<CO>.1` where `<CO>` is the cluster octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: `instadm`
8. At the prompt, enter the current password.

The **Installation Administrator Main Menu** appears.

9. Enter the number for **Configure Nationwide Cluster Information**.

The **Configure Nationwide Cluster Information** menu appears:

```
Configure Nationwide Cluster Information 1. List Zones in Cluster 2. Add Zone
to Cluster 3. Configure Nationwide Parameter 4. Define Nationwide DNS 5. List
available DNS root servers 6. Force DNS synchronization in the cluster 7. Force
Cluster DNS to the existing system Enter Selection: (1-8, q, ?) [q]
```

10. Enter the number for **Force DNS synchronization in the cluster**.

The following prompt appears:

```
Please enter the ZoneID's in this cluster (separated by space) and press Enter
```

11. Enter the ID of the zone.

A message appears, informing that the DNS has been synchronized successfully, followed by the **Configure Nationwide Cluster Information** menu:

```
Configure Nationwide Cluster Information 1. List Zones in Cluster 2. Add Zone
to Cluster 3. Configure Nationwide Parameter 4. Define Nationwide DNS 5. List
available DNS root servers 6. Force DNS synchronization in the cluster 7. Force
Cluster DNS to the existing system Enter Selection: (1-8, q, ?) [q]
```

12. Enter the number for **Add Zone to Cluster**.

The information about the number of zones in cluster appears:

```
Zones in cluster ucs10: - None - Enter zone ID to add. (1-56, q) [q]
```

13. Enter the number of the zone you want to add to the cluster.

The information about the number of the zones in the cluster appears:

```
Zones in cluster ucs10: 1. zone20 Zone 20 was added. Enter zone ID to add.
(1-56, q) [q]>
```



NOTE: If the zone DNS is not yet synchronized with the UCS DNS, you are not able to add a new zone to the cluster. Instead, an appropriate warning message appears.

14. Repeat [step 13](#) until all the zones are added to the cluster.

15. Log out of the UCS server by entering: `q` repeatedly until the logon prompt appears.

1.16

Enabling All Application Servers

You enable and disable application servers from their respective administration menus. Enabling application servers starts all of the processes necessary for the servers to function properly in the system.

Prerequisites: Before you enable all application servers after a fresh installation, perform the following database restorations in this order:

1. See [License Manager Post-Restoration Operations on page 64](#) for details regarding License Manager restoration scenarios. In case of the entire server replacement, no database restoration is required. In case of a component replacement and software re-installation, perform [License Manager – Restoring Data from Backup on page 214](#)
2. [UCS – Restoring Data from Backup on page 198](#)
3. [ZDS – Restoring Data from Backup on page 237](#)

Perform subsequent database restorations (do **not** restore Alias Server):

1. [AuC – Restoring Data from Backup on page 165](#)
2. [SSS – Restoring Data from Backup on page 186](#)
3. [UEM – Restoring Data from Backup on page 223](#)
4. [ZSS – Restoring Data from Backup on page 249](#)

Pre-configure Alias Server. See [AS – Configuring Application \(Windows Server 2016 Procedures\) on page 138](#). Reboot when the configuration is complete.

Pre-configure MultiCADI. See [MultiCADI – Application Configuration on page 148](#). Reboot when the configuration is complete.

Pre-configure ATR. See [ATR – Configuring Application on page 127](#). Reboot when the configuration is complete.

Log on to iGAS as sysadmin. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. Upon successful logon as sysadmin, verify that the **System Administrator Main Menu** appeared:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Enable all Application Servers**.



NOTE: Do **not** use fast enable for a fresh installation.

Process messages appear that indicate the application servers have been enabled, followed by the application server's Administration menu.

Postrequisites:

- Check data replication status between ZDS and UCS on both application servers. See [ZDS – Checking Data Replication Status on page 236](#).
- Perform ESU-based restoration for Alias Server. See [AS – Restoring Data from Backup on page 139](#). At this point, Alias Server switches to the **Enabled_And_Service_Up** state.
- Perform ESU-based restoration for MultiCADI. See [MCADI – Restoring Data from Backup on page 148](#).
- Perform ESU-based restoration for ATR. See [ATR – Restoring Data from Backup on page 129](#).

1.17

Updating the License on Legacy Red Hat AntiVirus Clients

Perform this process if AV Protection is installed in the system.



NOTE: Perform this procedure only if legacy Red Hat based application servers with ESET version 4 are present in the system.

This process is used for updating the AntiVirus Client license on Red Hat environment. The license update is performed by using the Enhanced Software Update (ESU) framework.



IMPORTANT: AntiVirus license cannot be updated on virtual containers that are currently shut down.



IMPORTANT: On HP DL360 Gen10 servers, you must use only the front horizontal USB 2.0 port located above the CD/DVD drive. If a serial adapter is inserted in this port, you must move it to another USB port or, if it is impossible, remove it. However, after the installation is complete, devices must be reconnected and rescanned by using iGAS. See "Rescanning the Devices by using iGAS" in the *Common Server and Client Platform Restoration*.

On HP DL360 Gen9, you can use any USB port, but you must first disable the USB 3.0 mode. See "Disabling USB 3.0 Support" in the *HP ProLiant DL360 Gen9 Server Platform Restoration* manual.

Procedure:

1. Obtain an AntiVirus License .iso image for Red Hat Clients:
 - a. Download the AntiVirus License .iso image for Red Hat clients from the link received from Motorola Solutions in "Enabling AntiVirus Server on CSMS" in the *Network Security* manual.
 - b. Copy the AntiVirus License .iso file to an NM Client. See [Updating AntiVirus Client License by Using Enhanced Software Update Framework on page 72](#).
2. Obtain the Network Security .iso image to be used in the upgrade process by performing the following actions:

The Network Security I .iso image (which is the .iso image start from AV_R09.01.01) can be found on the following USB media:

- Core Software without AIE without SSL/TLS
- Console Software non-SSL/TLS
- Console Software SSL/TLS
- Platform Software for NIR
- NMT Software

- a. Select the AV_R09.01.01.<XX>.iso image,
where <XX> is the number of the released Network Security I .iso image.
- b. Copy the .iso file to the NM Client hard drive.

3. On the NM Client PC, launch the ESU application, and log on with the **Upgrade** user role.
4. Perform [Updating AntiVirus Client License by Using Enhanced Software Update Framework](#) on page [72](#).

1.17.1

Updating AntiVirus Client License by Using Enhanced Software Update Framework

Perform this procedure to update the AntiVirus Client license by using the Enhanced Software Update Framework (ESU).

Prerequisites: Ensure that you have access to the *Enhanced Software Update* manual.

Obtain the Network Security I .iso image. See [Updating the License on Legacy Red Hat AntiVirus Clients](#) on page [71](#).

Launch the ESU application on the NM Client PC and log on with the **Upgrade** user role.

Procedure:

1. Copy the Network Security I .iso image to a convenient location on a local drive.
2. In the ESU, from the left-side menu, select **Upload Files**.
3. Click **Browse**, select the previously copied **Network Security I .iso** image, and click **OK**.
4. Click **Upload**.
5. Repeat [step 3 to step 4](#) to upload the .iso image that contains the AntiVirus license.
6. Multizone systems only: From the menu on the left, select **Configure Links**.
 **IMPORTANT:** For proper link configuration guidelines, see the *Enhanced Software Update* manual.
7. From the menu on the left, select **Distribution Sequence**.
8. Click **Distribute**.
9. From the menu on the left, select **Distribution View**.
10. Click **Start** and wait until the distribution finishes.
11. From the menu on the left, select **File Integrity**.
12. Click **Check integrity**.
13. Optional: If the files are out of sync, click **Synchronize**. Otherwise, proceed to [step 15](#).
14. Click **Start** and wait until the synchronization finishes.
15. From the menu on the left, select **Upgrade Composer**.
16. Click **Browse**.
17. In the **Choose File to Open** window, select the `D91_av_client_license_update.zip` file located on the Network Security I .iso image.
18. Click **Upload**.
19. From the table located in the middle of the page, select **Choose/Compose** for the file that has just been uploaded.
20. Click **Next → Create**.

The **Upgrade Player** window appears.

21. In the **Upgrade Player**, locate the task list defined for the **Deliver and install upgrade scripts** phase and click **Open** .
22. Click **Run**.
23. When the task list is completed successfully, select **Upgrade Player** again and run the task list defined in the second phase: **Installation of new license for AV Client**.

When all phases and task lists have successfully finished, the AntiVirus license is correctly installed on the system.

1.18

Server Password Change

For security purposes, use the following guidelines when creating administrator passwords to ensure that they are difficult for unauthorized users to guess.

The password must meet the following criteria:

- At least 15 characters, containing elements from the four types of characters:
 1. English uppercase letters
 2. English lowercase letters
 3. Westernised Arabic numerals 0, 1, 2 ... 9
 4. Special Characters !, @, #, \$...
- Differ from your logon name and any reverse or circular shift of your name
- Differ from the old password by at least three characters
- Have a minimum of eight different characters than old password
- Have no more than three consecutive repeating characters
- Have no more than four consecutive characters of the same class



CAUTION: The administrator password controls access to the administration menus. Keeping these menus secure is crucial, as the server's Administration menu provides access to vital network management functions. You should keep the administrator password secret and change it frequently.

1.18.1

Changing the Server Administrator Password

Perform this procedure to change the server administrator password.



NOTE: As a result of the following procedure, the iGAS sysadmin user passwords will be changed.

Prerequisites: Log on as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
```

```
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Unix Administration**.
3. Enter the number associated with **Change password**.
4. At the prompt, enter the current password.
5. At the prompt, enter the new password.
6. Enter the new password again.

A message appears stating that the password was changed successfully and you are returned to the previous menu.

 **NOTE:** If the second password does not match the first, an error message appears, and you are returned to the previous menu.

1.18.2

Changing the iLO User Password

Procedure:

1. Log on to iLO as the Administrator.
2. In the panel on your left-hand side, select **Administration** → **User Administration**.
3. In the **Local Users** section, select the check box next to the user whose password you want to change and click **Edit**.
4. In the **User Information** section, select the **Change password** check box if needed.
5. Type the new password in the **Password** and **Password Confirm** fields and click **Update User**.

 **NOTE:** It is not recommended to use the '=' sign when setting the iLO password.

1.19

Primary/Secondary Core Server – Installing and Configuring RSA Authentication Software

1.19.1

Installing and Configuring RSA Authentication Software on Linux Applications

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server for each application server installed on the Core Server. Follow "Clearing the Node Secret for a Particular Node" in the *Network Security* manual.

2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

1.19.2

Installing and Configuring RSA Authentication Software on Windows Applications

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server for each application server installed on the Core Server. Follow “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.

 **IMPORTANT:**
When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.
The RSA Agent installation should be performed after the promoting of Domain Controller.

Chapter 2

Domain Controller – Software Application Restoration (Windows 2016)

2.1

DC – Restoration Impact

No impact on services – remaining Domain Controllers will provide Active Directory services.

2.2

DC – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. Upon successful logon as `instadm`, the **Installation Administrator Main Menu** appears:

The **Installation Administrator Main Menu** appears.

Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:

2. Type the number associated with **Reinstall Applications** and press **ENTER**.

The list of available applications residing on the server appears.

3. Type **y** when the installer asks about reinstalling **Domain Controller**, and type **n** for the other applications.

The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.

4. Type **q** to log off the server.

5. Log in to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

System Administrator Main Menu

1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration

8. Application Isolation Management
Please enter selection (1-8, q) [q] :

6. Type the number associated with **Application Servers Boot/Reboot/Shutdown** and press ENTER.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q] :

7. Type the number associated with **Boot Application Servers** and press ENTER.

The **Boot Application** menu appears.

8. Type the number associated with **Domain Controller** and press ENTER.

You have booted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter **q** and press ENTER. Repeat this sequence until you log off the server.

2.3

DC – Performing Post-Restoration Operations

Process:

1. Open Remote Desktop session to the Domain Controller with installed Active Directory.
2. Log on as **admotosec**.
3. Open **Command Prompt**. Right-click **Start** and select **Command Prompt (Admin)**.
4. In the **Command Prompt** window, enter: `cd C:\AD_DS`
5. Optional: If the failed Domain Controller was the FSMO holder, see [Determining FSMO Role Owner on page 77](#) and [Seizing FSMO Roles on page 78](#).
6. Perform [Cleaning Up Metadata on page 79](#).
7. Log on to the newly reinstalled Domain Controller as **admotosec**.
8. Perform [Promoting Additional Domain Controllers on page 79](#).
9. Optional: If the recovered Domain Controller is DC01 in Primary Zone, transfer FSMO back to DC01. See [Transferring FSMO Roles on page 78](#).

2.4

Determining FSMO Role Owner

Perform this procedure to determine the current FSMO role owner.

Procedure:

1. Log on to any operational Domain Controller in the domain as a domain administrator.
2. On the Domain Controller, open a **Command Prompt** window. Right-click the Windows **Start** button and select **Command Prompt (Admin)**.
3. In the **Command Prompt** window, enter: `netdom query fsmo`

The Domain Controller computer names of the FSMO role owners are displayed.

2.5

Seizing FSMO Roles

Perform this procedure to seize FSMO roles from a failed Primary Domain Controller.

The FSMO roles are seized by the indicated Additional Domain Controller.

**NOTE:**

Use this procedure only if the Primary Domain Controller failed and is inaccessible.

If you want to transfer FSMO roles from a working Primary Domain Controller, perform [Transferring FSMO Roles on page 78](#).

Procedure:

1. Open a Remote Desktop session to any operational Domain Controller (DC).
2. Log on as the `admotosec` user.
3. On the DC, open a **Command Prompt** window. Right-click **Start** and select **Command Prompt (Admin)**.
4. In the **Command Prompt** window, enter: `cd C:\AD_DS`
5. Enter: `SeizeFSMO.bat <DC_NAME>` where `<DC_NAME>` is a fully qualified domain name of the DC that is to become the new FSMO holder.

Step example: `SeizeFSMO.bat z001dc02.zone1`

To prevent accidental seizing of FSMO roles held by a working Primary Domain Controller, the script first attempts to perform a safe FSMO roles transfer. When this transfer attempt fails, error messages appear.

Ignore the error messages starting with `ldap_modify-sW` error through Transfer of PDC FSMO failed, proceeding with seizure ...

Seizing begins only after this failed transfer attempt.

New FSMO holders are listed at the end of the script.

Postrequisites: Clean up the metadata. See [Cleaning Up Metadata on page 79](#).

2.6

Transferring FSMO Roles

Perform this procedure to transfer FSMO roles from a working Primary Domain Controller to an Additional Primary Controller. When FSMO role transfer is complete, the original Primary Domain Controller becomes an Additional Domain Controller, and the indicated Additional Domain Controller becomes the Primary Domain Controller.

Procedure:

1. Open a Remote Desktop session to any Domain Controller (DC).
2. Log on as the `admotosec` user.
3. On the DC, open a **Command Prompt** window. Right-click the Windows **Start** button and select **Command Prompt (Admin)**.
4. In the **Command Prompt** window, enter: `cd C:\AD_DS`
5. Enter: `MoveFSMO.bat <DC_NAME>` where `<DC_NAME>` is a fully qualified domain name of the DC that is to become the new FSMO holder.

Step example: `MoveFSMO.bat z001dc02.zone1`

New FSMO holders are listed at the end of the script.

2.7

Cleaning Up Metadata

Perform this procedure to clean up metadata. Metadata cleanup is required if any Domain Controller (DC) failed or was removed from the domain.

Procedure:

1. Open Remote Desktop session to an operational Domain Controller in the same Active Directory site where the failed Domain Controller is located.
-  **NOTE:** If both Domain Controllers in the same Active Directory site failed, open a Remote Desktop session to any operational Domain Controller.
2. Log on as the admotosec user.
3. Open a **Command Prompt** window. Right-click the Windows **Start** button and select **Command Prompt (Admin)**.
4. In the **Command Prompt** window, enter: `cd C:\AD_DS`
5. Enter: `RemoveMetadata.bat <DC_NAME>` where `<DC_NAME>` is a short name of a failed DC.

Step example: RemoveMetadata.bat z001dc02

A message appears informing that the metadata for the failed DC has been removed.

Postrequisites: Verify Active Directory Status. See [Active Directory Status Verification on page 80](#).

2.8

Promoting Additional Domain Controllers

Perform this procedure to install an Additional Domain Controller.

An Additional Domain Controller is any Domain Controller (DC) in an Active Directory domain that does **not** act as the Primary DC.

Prerequisites:

Ensure that the system time is accurately maintained. Active Directory strongly relies on proper time maintenance.

Ensure that a working NM Client PC is available to remotely log on to Domain Controllers and perform installation tasks.

Procedure:

1. Open a Remote Desktop session to the Domain Controller to be promoted as an Additional DC.
 **IMPORTANT:** During the DC promotion process, do **not** close the remote desktop connection and do **not** leave the console unattended. If you close the remote desktop connection, you must reconnect by using a web-based client. See [Accessing Virtual Machines with the Web-Based Client on page 140](#).
2. Log on as the local admotosec user.
3. In File Explorer, navigate to `C:\AD_DS`
4. Double-click `dcpromo_additional.bat`
5. Ensure that a correct Active Directory DNS domain name to join is displayed and press any key to continue.

6. At the prompt, create and enter the Directory Services Restore Mode administrator password. See [Password Requirements on page 80](#).

**NOTE:**

This password may be necessary for recovery purposes. Save it and keep it in a safe location.

The DSRM administrator password is stored locally on each Domain Controller. You can set a different DSRM administrator password on each Domain Controller.

7. In the **Windows Security** window, under **Enter my credentials on the authentic Windows sign-in screen**, click **OK**.

8. Press CTR + ALT + END and enter the domain administrator credentials.

Active Directory installation process begins.

At the end of the installation a message about successful installation appears and the system prompts you to restart the computer manually.



NOTE: During installation, only critical objects are replicated. Full replication only takes place after a reboot of the newly promoted Additional Domain Controller, and begins within 15 minutes from its restart.

9. Press any key to continue.

10. Restart the computer manually.

Postrequisites: After reboot, you may need to change your credentials for RDP logon. From now on, you need to log on as the domain administrator (and not the local administrator), using the `ad\admotosec` credentials.

2.8.1

Password Requirements

Passwords used in Active Directory have to meet the minimum requirements for a strong Windows password.

The default password policy is in effect. The password must meet the following criteria:

- Minimum password length: 8 characters
- Must contain one or more characters from at least 3 of the following categories:
 - Lowercase characters (a to z)
 - Uppercase characters (A to Z)
 - Digits (0 to 9)
 - Punctuation or special characters (for example: #, @, !, ;, or _)
- Must not contain more than two consecutive characters of the user account name or user full name
- Must not be one of the last 24 passwords

2.9

Active Directory Status Verification

The procedures covered in this section are used to assess the correctness of the Active Directory installation and its working condition.

2.9.1

Running Dcdiag Tests

This procedure describes how to run tests with the Dcdiag tool.

By using these tests, you can verify the status of the connectivity, topology, replication, and FSMO roles.

Perform Dcdiag tests at the end of an installation or recovery, and after configuration changes.

Prerequisites: Allow at least 15 minutes since the last installation or configuration changes, before you perform this procedure.

Procedure:

1. Log on to the Primary Domain Controller (Primary DC) in the Active Directory domain.
2. On the Primary DC, open a **Command Prompt** window. Right-click **Start** and select **Command Prompt (Admin)**.
3. In the **Command Prompt** window, enter the following commands:

```
dcdiag /test:connectivity /e
dcdiag /test:topology /e
dcdiag /test:kccevent /e
dcdiag /test:replications /e
dcdiag /test:verifyreplicas /e
dcdiag /test:KnowsOfRoleHolders /e
dcdiag /test:FSMOCHECK /e
```



NOTE: If an error occurs, wait additional 15 minutes, and then rerun this procedure.

2.9.2

Verifying Replication Status

Perform this procedure to verify the replication status.



IMPORTANT: Do **not** start joining PCs to the Active Directory domain unless the verification is completed successfully.

Procedure:

1. Log on to the Primary Domain Controller in the Active Directory domain.
2. On the desktop, double-click **Replication Status**.

The **Replication Status** window appears.

Figure 4: Replication Status Log

Replication Status										
showrep_COLUMNS	Destination DSA Site	Destination DSA	Naming Context	Source DSA Site	Source DSA	Transport Type	Number of Failures	Last Failure Time	Last Success Time	Last Fi
showrep_INFO	zone2	Z002DC02	DC=ad,DC=zone2	zone2	Z002DC01	RPC	0	0	2018-04-24 15:44:19	0
showrep_INFO	zone2	Z002DC02	CN=Configuration,DC=ad,DC=zone2	zone2	Z002DC01	RPC	0	0	2018-04-24 15:44:27	0
showrep_INFO	zone2	Z002DC02	CN=Schema,CN=Configuration,DC=ad,DC=zone2	zone2	Z002DC01	RPC	0	0	2018-04-24 15:43:59	0
showrep_INFO	zone2	Z002DC01	DC=ad,DC=zone2	zone2	Z002DC02	RPC	0	0	2018-04-24 15:43:23	0
showrep_INFO	zone2	Z002DC01	CN=Configuration,DC=ad,DC=zone2	zone2	Z002DC02	RPC	0	0	2018-04-24 15:44:12	0
showrep_INFO	zone2	Z002DC01	CN=Schema,CN=Configuration,DC=ad,DC=zone2	zone2	Z002DC02	RPC	0	0	2018-04-24 15:43:04	0



NOTE: Values in the **Replication Status** window are not refreshed automatically. You can obtain new values by closing and reopening this application.

3. Ensure that the following conditions are met:

- In the **showreplCOLUMNS** column, **only** showrepl_INFO records appear and there are **no** showrepl_ERROR records.
- In the **Number of Failures** column, **only** zeroes appear.
- In the **Last Failure Time** column, **only** zeroes appear.
- In the **Last Success Time** column, **no** (never) values appear ((never) indicates a replication failure). **Example:** 2015-02-18 13:12:53 is a correct value.

4. Perform one of the following actions:

If...	Then...
If any of the conditions from step 3 are not met,	reopen the application after 15 minutes and perform verification once again.
If all the conditions from step 3 are met,	perform the following actions: <ol style="list-style-type: none">a. Close the Replication Status application.b. Close the Replication Status console window by pressing ENTER.

Chapter 3

Core Security Management Server – Software Application Restoration

3.1

CSMS – Pre-Restoration Checks

 **IMPORTANT:** Before starting the restoration procedure, you must check for any new Motorola Solutions Technical Notification (MTN).

3.2

CSMS – Software Application Restoration Reference

The following section describes the backup and restoration procedures for the elements of the Core Security Management Server (CSMS).

Table 6: Core Security Management Server – Restoration Reference

This table contains references to procedures to be performed to restore and back up the software and data. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Action	Reference	Done
Software Restoration by using a switchover	CSMS – Restoring Software by Using a Switchover on page 84	
Software Restoration by using UIS	CSMS – Restoring Application on page 84 CSMS – Switching Server to Active State on page 85 CSMS – Starting Up the ESU Application on page 86 CSMS – Uploading a Backup File to UIS on page 87 CSMS – Restoring Data from Backup on page 88 CSMS – Re-activating the Restored AV CSMS on page 88 CSMS – Installing and Configuring RSA Authentication Software on page 89	
Full Software Restoration without any backup stored	CSMS – Restoring Application on page 84 CSMS – Configuring the AntiVirus Server on page 89 CSMS – Installing and Configuring RSA Authentication Software on page 89	
Backing up the application	CSMS – Data Backup on page 89	

 **NOTE:** After a successful restoration, the application is joined to the Active Directory domain. To access the application, you must log on to it by using appropriate credentials. See “Logging On to Domain Member PCs” in the *Active Directory* manual.

3.3

CSMS – Restoring Software by Using a Switchover

Process:

1. Switch the Standby AntiVirus Core Security Management Server (CSMS) server to Active redundancy state by using Administration command: 2: Switch to Active. See [Administering the Active/Standby AV CSMS on page 85](#).
The new Active AV CSMS will use the last synchronized database (synchronization occurs one a day).
2. Restore the failed CSMS application. See [CSMS – Restoring Application on page 84](#).
3. Create a backup of the database of the new Active AV CSMS by using Administration command: 6 : Sync database. See [Administering the Active/Standby AV CSMS on page 85](#).
4. On the restored (now Standby) AV CSMS, sync the database by using Administration command: 6 : Sync database. See [Administering the Active/Standby AV CSMS on page 85](#).
5. Switch the restored (now Standby) AV CSMS server to Active redundancy state by using Administration command: 2: Switch to Active. See [Administering the Active/Standby AV CSMS on page 85](#).
6. On the Active AV CSMS, install and configure the RSA Authentication Software. See [CSMS – Installing and Configuring RSA Authentication Software on page 89](#).

3.4

CSMS – Restoring Application

Prerequisites: Log on to iGAS as **instadm**. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)



NOTE: Skip this procedure if the Core Security Management Server (CSMS) virtual machine works properly.

Procedure:

1. Enter the number for **Reinstall Applications**.
The list of available applications residing on the server appears.
2. Enter: **y** when the installer asks about reinstalling Core Security Management Server, and enter: **n** for other applications.
The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.
3. Log off from the server by entering: **q**
4. Log on to iGAS as **sysadmin**.
The **System Administrator Main Menu** appears.
5. Enter the number for **Application Servers Boot/Reboot/Shutdown**.
The **Application Servers Boot/Reboot/Shutdown** menu appears.
6. Enter the number for **Boot Application Servers**.

7. Enter the number for Core Security Management Server.
- You have booted the application.
8. Enter: q repeatedly until you log off the server.

3.5

CSMS – Switching Server to Active State

Procedure:

Switch the AntiVirus Core Security Management Server (CSMS) server to Active redundancy state by using Administration command: 2: Switch to Active. See [Administering the Active/Standby AV CSMS on page 85](#).

3.5.1

Administering the Active/Standby AV CSMS

Procedure:

1. Log on to the NM Client by using the local motosec account.
2. Open a Remote Desktop connection to the Active/Standby AV CSMS by using the motosec account on the remote machine.
3. On a Desktop, right-click the **Manage_CSMS** shortcut, and select **Run as administrator**.
A list of options appears.
4. Enter the number for the command you want to perform.

For the full list of commands and their descriptions, see [Active/Standby AV CSMS Administration Commands on page 85](#).

3.5.2

Active/Standby AV CSMS Administration Commands

When connecting to the Active or Standby AntiVirus Core Security Management Server (AV CSMS), a list of commands displays detailing actions which can be performed.

Table 7: Administrator: Manage CSMS – Commands

Command	Server	Description/Output
1: Redundancy Status	Active AV CSMS	Output: Current redundancy state: Active
	Standby AV CSMS	Output: Current redundancy state: Standby
2: Switch to Active	Active AV CSMS	Does not trigger any action.
	Standby AV CSMS	Triggers a switchover to the Active state. The previous Active

Command	Server	Description/Output
		AV CSMS switches to Standby automatically within 1 minute.
		 IMPORTANT: Database synchronization between Active AV CSMS and Standby AV CSMS takes place once a day (scheduled). During the switchover, the last synced database is used.
3: Switch to Standby	Active AV CSMS	Switches to Standby state.
	Standby AV CSMS	Does not trigger any action.
4: Backup DB to file	Active AV CSMS	Backs up the database to a file.
5: Restore DB from file	Active AV CSMS	Restores the database from a file.
6: Sync database	Active AV CSMS	Creates a database backup to synchronize with Standby AV CSMS.
	Standby AV CSMS	Downloads the database from Active AV CSMS and restores it.
7: Sync signatures	Active AV CSMS	Creates a backup of signatures to synchronize with Standby AV CSMS.
	Standby AV CSMS	Downloads signatures from Active AV CSMS and restores the server.
8: Restart ESET PROTECT service	Active AV CSMS	Restarts the ESET PROTECT service.
9: Restart Apache HTTP Proxy	Active/Standby AV CSMS	Restarts the Apache HTTP proxy service.
0: Exit	Active/Standby AV CSMS	Exits the program.

3.5.3

CSMS – Starting Up the ESU Application

Prerequisites: Log on to the NM Client by using the local motosec account.

Procedure:

1. Open a web browser (Chromium) and enter the following URL address: <https://master-uis.ucs/ui>



IMPORTANT:

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS01: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, enter a user name associated with the **Backup** user role.

3. In the **Password** field, enter the password associated with the user.

4. Click **Log in**.

You are logged on to the Enhanced Software Update (ESU) application and connected to the Master UIS. The start page of the ESU tool appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [CSMS – Uploading a Backup File to UIS on page 87](#). Otherwise, if the backup file already is in the UIS backup storage, continue to [CSMS – Restoring Data from Backup on page 88](#).

3.5.4

CSMS – Uploading a Backup File to UIS

Prerequisites: Log on to the ESU with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the ESU.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.



NOTE: If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the ESU, select **Upload Files**.

The **Upload Files** screen appears.

2. Click **Browse**.

3. In the window that appears, select your backup file. Click **OK**.



NOTE: The backup file is named `zone<XX>csmsdb<YY>_<timestamp>` where:

`<XX>` is the zone ID

`<YY>` is 01 for csms00 or 02 for csms02

`<timestamp>` is a date and time written as one row of digits with the format `<yyyyymmddhhmm>`

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

5. Click **Analyze Uploaded File**.

If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

3.5.5

CSMS – Restoring Data from Backup

Prerequisites:

You must be logged in to the Enhanced Software Update (ESU) application on the Master UIS, with the **Backup** user role.

A data backup file must be available.

The application server that you want to restore must be enabled. If the application server is disabled, the restoration fails. If the application server is not enabled, see [CSMS – Re-activating the Restored AV CSMS on page 88](#).

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named zone<XX>csmldb<YY>_<timestamp>

where:

<XX> is the zone ID

<YY> is 01 for csms00 or 02 for csms02

<timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

3.5.6

CSMS – Re-activating the Restored AV CSMS



IMPORTANT: Clients that can connect to the restored AntiVirus (AV) Core Security Management Server (CSMS) between steps [CSMS – Switching Server to Active State on page 85](#) and [CSMS – Restoring Data from Backup on page 88](#) are doubled in the ESMC Web Console, under the **Computers** section. To delete unnecessary Clients, see "Removing Unneeded AV Clients on ESET Security Management" in the *Network Security* manual. Removing Unneeded AV Clients is possible after a minimum of 1 day after the unneeded clients lost connection to the AV server.

Procedure:

After restoration from the Enhanced Software Update (ESU), execute **Switch to Active** on the restored AV CSMS. See [Administering the Active/Standby AV CSMS on page 85](#).

3.5.7

CSMS – Installing and Configuring RSA Authentication Software

Procedure:

1. Clear 2FA Secret key on the RSA server. See the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.



IMPORTANT:

When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

The RSA Agent installation should be performed after the promoting of Domain Controller.

3.6

CSMS – Configuring the AntiVirus Server

For information on AntiVirus server configuration, see "AntiVirus Software Installation and Configuration" in the *Network Security* manual.

3.7

CSMS – Data Backup

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.



IMPORTANT: Creating a backup is critical because it stores ESET AntiVirus client licenses.

3.7.1

CSMS – Starting Up the ESU Application

Prerequisites: Log on to the NM Client by using the local motosec account.

Procedure:

1. Open a web browser (Chromium) and enter the following URL address: <https://master-uis.ucs/ui>

IMPORTANT:

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
 - For MUIS01: <https://ucs-muis02.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Enhanced Software Update (ESU) application and connected to the Master UIS. The start page of the ESU tool appears showing a menu at the left and a welcome message.

3.7.2

CSMS – Configuring Backup

Prerequisites: You must be logged on to the Enhanced Software Update (ESU) application with the **Backup** user role.

Procedure:

1. From the left-hand side menu on the ESU application, select **Backup Configuration**.

A table appears showing all applications that support backup in all zones residing in the cluster handled by ESU.

2. Perform one of the following actions:

- If you want to save the backup file in the local storage of the zone UIS, select the check box of the **csms_active** application in the **Add To Backup/Restore** column.
- If you want to save the backup file in the central storage of the Master UIS, select the check box of the **csms_active** application in the **Use Central Storage** column. Ensure that you select the check box for the CSMS in the correct zone.

Ensure that you select the check box for the CSMS application in the correct zone.



NOTE: You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used when you perform data restoration.

3. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

Perform one, or both of the following actions:

- If you want to create a backup file immediately, see [CSMS – Backing Up Data On-Demand on page 90](#).
- If you want to create a scheduled backup task running at regular intervals, see [CSMS – Scheduling Backup on page 91](#).



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

3.7.3

CSMS – Backing Up Data On-Demand

Prerequisites: You must be logged on to the Enhanced Software Update (ESU) application on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. From the left-hand side menu of the ESU application, select **Backup**.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **csms_active** application in the relevant zone, click **Run**.

3. Optional: You can run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.



NOTE: When the backup task is initiated, the ESU tool finds out whether any of the redundant applications are active. If there is an active application, the backup is performed for this application. If none of the redundant applications are active, the backup fails.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites:

- If you want to create a scheduled backup task running at regular intervals, see [CSMS – Scheduling Backup on page 91](#).
- If you want to save the backup file on the NM Client PC, see [CSMS – Downloading a Backup File to the NM Client PC on page 92](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

3.7.4

CSMS – Scheduling Backup

Prerequisites: You must be logged on to the Enhanced Software Update (ESU) application on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. From the left-hand side menu of the ESU application, select **Scheduled Backup**.
A table showing a list of scheduled backups appears. The date and time of the Master UIS is displayed below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Perform the following actions:
 - a. In the **Name** field, type a name for the scheduled backup task.
 - b. Click the browse button to select the zone, the sub-domain, and the application for which the scheduled backup must be set up.
 - c. In the list that appears, in the row containing the **csms_active** application in the relevant zone, click **Select** to select a zone, a subdomain, and an application at the same time.
 - d. From the **Day** drop-down list, select a week day, or select **DAILY**.
 - e. From the **Hour** drop-down list, select at which hour the backup must run.
 - f. From the **Minute** drop-down list, select at which minute the backup must run.
 - g. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

4.
 - If your scheduled backup file has been created, and you want to save it on the NM Client PC, see [CSMS – Downloading a Backup File to the NM Client PC on page 92](#).
 - If your scheduled backup file has been created, and you do not want to save it on the NM Client PC, you do not have to do anything.

Postrequisites:

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

3.7.5

CSMS – Downloading a Backup File to the NM Client PC

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

You must be logged in to the Enhanced Software Update (ESU) application with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

Procedure:

1. From the left-hand side menu of the ESU application, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.
2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `zone<XX>_csmldb_01_<timestamp>.tar.gz` where:
 - <XX> is the zone ID
 - <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>You can download only one file at a time.
A warning appears asking whether you want to save the file.
3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Chapter 4

UIS – Software Application Restoration

This table contains references to procedures to be performed to restore and back up the UIS application server software and data. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 8: UIS – Backup and Restoration Checklist

Action	Reference	Done
Restoring the application	<p>UIS – Restoration Impact on page 93</p> <p>UIS – Pre-Restoration Checks on page 94</p> <p>UIS – Restoring Software on page 94</p> <p>Depending on which type of UIS you are restoring, refer to the following sections:</p> <ul style="list-style-type: none"> • UIS – Restoring Data on Zone UIS on page 99 • UIS – Restoring Data on a Redundant Master UIS on page 95 • UIS – Restoring Data on Non-Redundant Master UIS on page 97 <p>UIS – Installing and Configuring RSA Authentication Software on page 101</p> <p>UIS – Post-Restoration Checks on page 102</p>	
Backing up the application	UIS – Backing Up Data on page 102	

4.1

UIS – Restoration Impact

Table 9: UIS – Restoration Impact

Action	Service Affected	Service Downtime
Zone UIS restoration	Content of software storage, log archives, and backup storage is lost.	
Master UIS restoration	<ul style="list-style-type: none"> • Users and passwords are lost. • Backup configuration is lost. • Scheduled backup configuration is lost. • Upgrade configuration is lost. • Content of software storage and backup storage is lost. 	

Related Links

[UIS – Software Application Restoration](#) on page 93

4.2

UIS – Pre-Restoration Checks

Before you do any restoration tasks, make sure that you are familiar with the guidelines described in the *Common Server and Client Platform Restoration* manual.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.3

UIS – Restoring Software

4.3.1

UIS – Restoring Application

Prerequisites: Ensure that the server is on.

Procedure:

1. On the NM Client PC, start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter:
10.<Z0>.233.222

where <Z0> is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is
10.<Z0>.233.223

where <Z0> is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: motorola
8. At the prompt, enter the password.
9. Enter the number for the Primary or Secondary Core Server to which you want to log on.

10. At the logon prompt, enter: `instadm`
11. At the prompt, enter the current password.
The **Installation Administrator Main Menu** appears.
12. Enter the number associated with **Reinstall Applications**.
The list of available applications residing on the server appears.
13. Enter `y` when the installer prompts you to re-install UIS and enter: `n` for other applications.
The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.
14. Log off the server by entering `q`
15. Log on to iGAS as `sysadmin`.
The **Application Servers Administration Menus** appears.
16. Enter the number for **Application Servers Boot/Reboot/Shutdown**.
17. Enter the number for **Boot Application Servers**.
18. Enter the number associated with UIS.
You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.
19. Enter: `q` repeatedly until you log off from the server.

4.3.2

UIS – Configuring Application

The application does not require any configuration after restoration.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.4

UIS – Restoring Data on a Redundant Master UIS

The procedures below describe a situation when there are two Master UIS servers.



NOTE: Always reinstall a standby Master UIS.

4.4.1

Checking Reinstalled Application Availability in ESU

Prerequisites: Before you can start this procedure, you must be logged on to the NM Client PC. Before taking any upgrade actions check the availability of the reinstalled application as described below. Before you can start this procedure, you must be logged in to the Upgrade Console with the **Admin** user role.

Procedure:

1. Open the Internet browser and enter the following URL address: <https://master-uis.ucs/ui>.

 **IMPORTANT:** In general you must always log in to the Master UIS. The ability to back up and restore is provided by the Master UIS only.

2. In the **User name** field, type a user name associated with the **Admin** user role.
3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

5. Select **Registered Agents** in the menu at the left.
6. Expand the tree in the **Registered agents** field.
7. Verify whether reinstalled application is displayed. If not, verify a network connection.

 **NOTE:** It may take few minutes to show on a web page. You can use **Refresh now** button to refresh displayed content manually.

4.4.2

Checking File Integrity

Prerequisites: Launch Upgrade Console on the NM Client PC. Log on with the **Upgrade** user role.

Procedure:

1. Select **File Integrity** in the menu at the left.

A table appears showing a list of applications and their checking status.

Figure 5: File Integrity Page

Zone	Subdomain	Application Name	Checking	Status	Details	Show
zone1		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone2		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone3		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone4		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone5		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone6		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone7		uis01	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone1		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone2		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone3		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone4		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone5		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone6		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>
zone7		uis02	N/A	In Synch	<input type="button" value="Details"/>	<input type="button" value="Show"/>

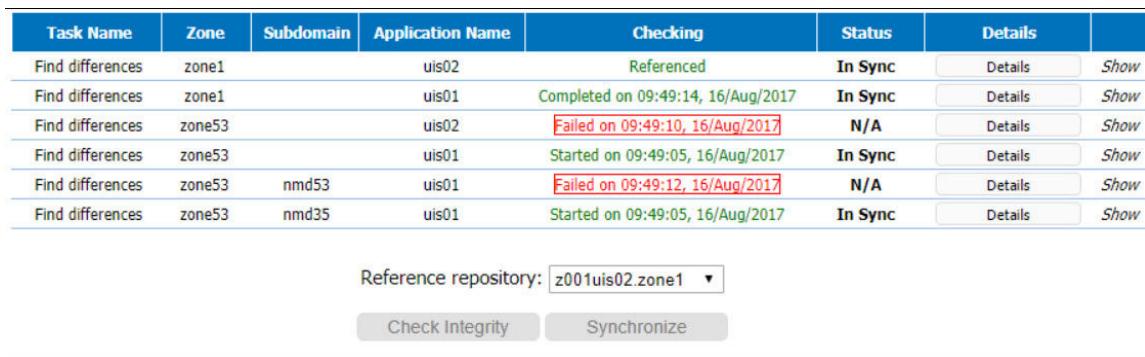
Reference repository:

2. From the **Reference repository** drop-down list, select the relevant software storage that all other software storages are checked against. Click **Check integrity**.

 **NOTE:** If the files are large, the integrity check can take up to 5 minutes.

The **Checking** column shows a time stamp for the check. In the **Checking** column of the reference repository, the status **Referenced** is shown. The **Status** column shows whether the files on a given UIS are in sync or not in sync with the files in the reference repository.

Figure 6: Check Integrity Page – Integrity Check in Progress



The screenshot shows a table with columns: Task Name, Zone, Subdomain, Application Name, Checking, Status, and Details. The table lists several tasks, some of which have failed. Below the table is a dropdown menu for the Reference repository, a 'Check Integrity' button, and a 'Synchronize' button.

Task Name	Zone	Subdomain	Application Name	Checking	Status	Details	Show
Find differences	zone1		uis02	Referenced	In Sync	Details	Show
Find differences	zone1		uis01	Completed on 09:49:14, 16/Aug/2017	In Sync	Details	Show
Find differences	zone53		uis02	Failed on 09:49:10, 16/Aug/2017	N/A	Details	Show
Find differences	zone53		uis01	Started on 09:49:05, 16/Aug/2017	In Sync	Details	Show
Find differences	zone53	nmd53	uis01	Failed on 09:49:12, 16/Aug/2017	N/A	Details	Show
Find differences	zone53	nmd35	uis01	Started on 09:49:05, 16/Aug/2017	In Sync	Details	Show

Reference repository: z001uis02.zone1 ▾

Check Integrity Synchronize

- View the detailed file integrity information about the applications which are out of sync. In the **Details** column, click **Details**.

The details tell which files must be deleted or added to make the files on a UIS in sync with the files in the reference repository.

- If the files are out of sync, click **Synchronize**.

A table appears showing the synchronization tasks, and the related source and destination Upgrade Install Servers.

- Click **Start**.

Result: The synchronization task is executed. The **Status** and **Progress** columns show status and progress of the task.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.5

UIS – Restoring Data on Non-Redundant Master UIS

A restoration is done on an active Master UIS. To restore data, you have to upload a backup file to the UIS backup storage. Proceed to the following sections.

4.5.1

Uploading Files

Prerequisites:

Launch the Upgrade Console application on the NM Client PC.

Log on with the **Backup** or **Upgrade** user role.

Procedure:

- Select **Upload Files** in the menu at the left.

A page appears providing access to upload and analyze files.



NOTE: The first time you open this page, you may be asked to accept one or two certificates. After accepting the certificates once on a particular NM Client PC, such prompts do not appear any more.

2. Click **Browse**.
3. Select the relevant file in the window that appears, and click **OK**.
4. Click **Upload**.



IMPORTANT: Stay on the **Upload Files** page while the software is being uploaded and analyzed. Changing the page or closing the browser before the process completes may damage the uploaded software.

5. Optional: To view details of the upload, under the **Details** column, click **show**.

Result: If the file format is correct, the file is placed in the proper UIS storage (backup storage or software storage).

Postrequisites:

- If the uploaded file is a backup file, you can now use it for restoration of data, if you have done one of the following:
 - You have placed the file on the Master UIS and selected the **Use Central Storage** check box for the relevant application.
 - You have placed the file on the local UIS, and the **Use Central Storage** check box is not selected for the application to be restored.
- If it is an ISO image, configure links between the zones in your system, so that you can distribute that ISO image.

4.5.2

Restoring a Database on a Non-Redundant Master UIS

Use this procedure during data restoration on a non-redundant Master UIS.

Prerequisites: Upload a backup file that you want to use during restoration (see [Uploading Files on page 97](#)). Log on to the Upgrade Console with the **Admin** user role.

Procedure:

1. Select **Master UIS Administration** in the menu at the left.
A page appears providing access to administration and debug fields.
2. In the **Database Administration** section, click **Refresh Filename**.
The name of a previously uploaded backup file appears.
3. In the **Database Administration**, click **Restore**.
The **Are you sure to Restore Master UIS** message appears. Confirm to proceed.
 **NOTE:** It takes about 20 minutes for all agents to register on the Master UIS.
4. Select **Sign out**.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.6

UIS – Restoring Data on Zone UIS

4.6.1

Checking Reinstalled Application Availability in ESU

Prerequisites: Before you can start this procedure, you must be logged on to the NM Client PC. Before taking any upgrade actions check the availability of the reinstalled application as described below. Before you can start this procedure, you must be logged in to the Upgrade Console with the **Admin** user role.

Procedure:

1. Open the Internet browser and enter the following URL address: <https://master-uis.ucs/ui>.
-  **IMPORTANT:** In general you must always log in to the Master UIS. The ability to back up and restore is provided by the Master UIS only.

2. In the **User name** field, type a user name associated with the **Admin** user role.
3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

5. Select **Registered Agents** in the menu at the left.
6. Expand the tree in the **Registered agents** field.
7. Verify whether reinstalled application is displayed. If not, verify a network connection.

 **NOTE:** It may take few minutes to show on a web page. You can use **Refresh now** button to refresh displayed content manually.

4.6.2

Checking File Integrity

Prerequisites: Launch Upgrade Console on the NM Client PC. Log on with the **Upgrade** user role.

Procedure:

1. Select **File Integrity** in the menu at the left.

A table appears showing a list of applications and their checking status.

Figure 7: File Integrity Page

Zone	Subdomain	Application Name	Checking	Status	Details	Show
zone1		uis01	N/A	In Synch	Details	Show
zone2		uis01	N/A	In Synch	Details	Show
zone3		uis01	N/A	In Synch	Details	Show
zone4		uis01	N/A	In Synch	Details	Show
zone5		uis01	N/A	In Synch	Details	Show
zone6		uis01	N/A	In Synch	Details	Show
zone7		uis01	N/A	In Synch	Details	Show
zone1		uis02	N/A	In Synch	Details	Show
zone2		uis02	N/A	In Synch	Details	Show
zone3		uis02	N/A	In Synch	Details	Show
zone4		uis02	N/A	In Synch	Details	Show
zone5		uis02	N/A	In Synch	Details	Show
zone6		uis02	N/A	In Synch	Details	Show
zone7		uis02	N/A	In Synch	Details	Show

Reference repository: [Choose One](#)[Check Integrity](#)[Synchronize](#)

- From the **Reference repository** drop-down list, select the relevant software storage that all other software storages are checked against. Click **Check integrity**.



NOTE: If the files are large, the integrity check can take up to 5 minutes.

The **Checking** column shows a time stamp for the check. In the **Checking** column of the reference repository, the status **Referenced** is shown. The **Status** column shows whether the files on a given UIS are in sync or not in sync with the files in the reference repository.

Figure 8: Check Integrity Page – Integrity Check in Progress

Task Name	Zone	Subdomain	Application Name	Checking	Status	Details	Show
Find differences	zone1		uis02	Referenced	In Sync	Details	Show
Find differences	zone1		uis01	Completed on 09:49:14, 16/Aug/2017	In Sync	Details	Show
Find differences	zone53		uis02	Failed on 09:49:10, 16/Aug/2017	N/A	Details	Show
Find differences	zone53		uis01	Started on 09:49:05, 16/Aug/2017	In Sync	Details	Show
Find differences	zone53	nmd53	uis01	Failed on 09:49:12, 16/Aug/2017	N/A	Details	Show
Find differences	zone53	nmd35	uis01	Started on 09:49:05, 16/Aug/2017	In Sync	Details	Show

Reference repository: [z001uis02.zone1](#)[Check Integrity](#)[Synchronize](#)

- View the detailed file integrity information about the applications which are out of sync. In the **Details** column, click **Details**.

The details tell which files must be deleted or added to make the files on a UIS in sync with the files in the reference repository.

- If the files are out of sync, click **Synchronize**.

A table appears showing the synchronization tasks, and the related source and destination Upgrade Install Servers.

5. Click Start.

Result: The synchronization task is executed. The **Status** and **Progress** columns show status and progress of the task.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.7

Generating and Installing SSH Keys

Generate the SSH keys on an active Master UIS to enable secure UIS-UIS traffic.

Perform this procedure in the following situations:

- After installing the system.
- After reinstalling an active or standby UIS in any zone in the cluster.



IMPORTANT: If you reinstall a UIS after a previous successful SSH key generation and distribution, perform this procedure again, even if the validation status shown on the **Registered Agents** page displays **SUCCESS**.

- After adding a zone to the system.

Prerequisites: Launch the Upgrade Console application on the NM Client PC. Log on with the **Admin** user role.

Procedure:

1. From the **Administrator Menu**, click **Master UIS Administration**.
2. On the **Master UIS Administration** page, in the **Key Administration** section, click **Run**.
3. Optional: View the tasks involved in the process. In the **Details** column, click **Show**.

Result: An indicator shows that the tasks involved in SSH keys generation and installation are running. The **Status** column of the **Key Administration** table shows the start and completion of the task.

4.8

UIS – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.



IMPORTANT: When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.9

UIS – Post-Restoration Checks

There are no specific post-restoration checks.

Related Links

[UIS – Software Application Restoration](#) on page 93

4.10

UIS – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.



NOTE: Only an active Master UIS can be backed up. The following procedures reflect this scenario.

4.10.1

Starting Up the Upgrade Console

You want to backup or restore data, to upgrade the system, or to handle administrative tasks related to the Upgrade Console, for instance, administration of users.

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the Internet browser and enter the following URL address: <https://master-uis.ucs/ui>



IMPORTANT:

In general, you must always log on to the Master UIS using the URL address: <https://master-uis.ucs/ui>

The backup, restore, and upgrade operations are only provided by the Master UIS. However, in case of a Master UIS switchover, the two following URLs must be used:

- For MUIS01:
<https://ucs-muis01.ucs/ui>
- For MUIS02:
<https://ucs-muis02.ucs/ui>

2. In the **User name** field, type your user name.

User names are associated with specific roles. The roles are:

- **Admin** – the user has access to administrative tasks
- **Backup** – the user has access to backup and restoration tasks
- **Upgrade** – the user has access to software update tasks

- **Upgrade Observer** – the user has access to follow the progress of the software update tasks



NOTE:

There are predefined users for each user role:

- Admin role: admin
- Backup role: backup
- Upgrade role: upgrade
- Upgrade Observer role: observer

3. In the **Password** field, type the password associated with the user name.
4. Click **Log in**.

Result: You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

4.10.2

Configuring Backups

You can configure backups to be able to back up data on demand, to create a scheduled backup task that runs at regular intervals, or to restore data.

Prerequisites: Launch the Upgrade Console application on the NM Client PC. Log on with the **Backup** user role.

Procedure:

1. From the left-hand menu, select **Backup Configuration**.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

Figure 9: Backup Configuration Page

Backup Configuration Wizard						
Zone	Subdomain	Application Name	Add To Backup/Restore	Use Central Storage	Use Storage PC	
zone13		alias_active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		atr01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		auc_active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		master_uis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		mcadi01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		mtig_e101	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
zone13		sss01	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
zone13		ucs01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		uem01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		zc01	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
zone13		zc02	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
zone13		zds01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone13		zss01	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
zone21		alias_active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone21		atr01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone21		mcadi01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone21		pdr_active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone21		sdr_active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone21		uem01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
zone21		zc01	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

<<< 1 2 >>

Apply changes

2. If you want to save the backup file in the local storage of the zone UIS, in the **Add To Backup/Restore** column select the check boxes of the relevant application servers.

Saving the backup file in the local storage means that the backup file is transferred to the Home UIS of the agent (see the **Registered Agents** page available when you are logged in with the **Admin** user role). If there is a second UIS in the zone, the backup file is also transferred to this UIS.

 **NOTE:** You can save the backup file in the local as well as central storage. If the backup file is saved in both storages, the backup file from the central storage is used when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check boxes of the relevant applications in the **Use Central Storage** column.

 **NOTE:** For redundant applications, the active application is indicated by adding **_active** to the name.

4. If you want to save the backup file in the Storage PC, select the check boxes of the relevant applications in the **Use Storage PC** column.

 **NOTE:**

The backup file is saved on all Storage PCs.

You can check the **Use Central Storage** option only when the **Add to Backup/Restore** option is selected. The **Use Storage PC** option can be selected only when the **Use Central Storage PC** option is selected and there is at least one Storage PC assigned in the system.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites: To create a backup file, run a backup task on demand, or configure a scheduled backup that runs automatically at specified intervals.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

4.10.3

Backing Up the Master UIS

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.



NOTE: You can only back up an active Master UIS.

Prerequisites:

Configure a backup. See [Configuring Backups on page 103](#).

Log on to the Upgrade Console on the Master UIS with the **Backup** user role.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The Backup page appears showing applications selected for backup.
2. In the **Action** column of the **master_uis** application, click **Run**.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task completes. The backup file is created in the local storage of the application. Then it is transferred to the backup storage directory on the Master UIS. If the **Use Central Storage** option was chosen, then the backup file is transferred to central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, then it is transferred to all assigned Storage PCs as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept (if the **Allow File Rotation** option is not selected).

Postrequisites: Perform one of the following actions:

- If you want to create a scheduled backup task running at regular intervals, continue to [Scheduling Backups on page 106](#).
- If you want to download the backup file from UIS backup storage, continue to [Downloading Backup Files on page 107](#).
- If the backup file you just created satisfies your needs for backup, you do not have to take any further actions regarding backup.

4.10.4

Scheduling Backups

A data backup must be created regularly according to the backup frequency defined for an application. If you want to back up data automatically on a regular basis, you should set up a scheduled backup.



NOTE:

It is highly recommended not to schedule backups for all entities to run at the same time.

SSS and ZSS statistics data collection runs every hour between XX:00 and XX:15, so the recommended time for all scheduled SSS and ZSS backups is at XX:45.

Prerequisites:

Launch the Upgrade Console application on the NM Client PC.

Log on with the **Backup** user role.

Procedure:

1. From the menu at the left, select **Schedule Backup**.
A table appears showing a list of scheduled backups.
2. On the **Schedule Backup** page, click **New**.
A page appears allowing you to define the scheduled backup.

Figure 10: New Backup Schedule Page

Name	<input type="text"/>
Zone	<input type="text"/> <input type="button" value="Add"/>
Subdomain	<input type="text"/> <input type="button" value="Add"/>
Application Name	<input type="text"/> <input type="button" value="Add"/>
Recurrence	<input type="text" value="DAILY"/> <input type="button" value="▼"/>
Day	<input type="text" value="Choose One"/> <input type="button" value="▼"/>
Hour	<input type="text" value="0"/> <input type="button" value="▼"/>
Minute	<input type="text" value="0"/> <input type="button" value="▼"/>
Interval	<input type="radio"/> 6h <input type="radio"/> 12h <input checked="" type="radio"/> 24h
<input type="button" value="Back"/> <input type="button" value="Submit"/>	

3. Specify the backup schedule parameters:
 - a. In the **Name** field, enter a name for the scheduled backup task.
 - b. Click any of the **Add** buttons.
 - c. In the list of applications, click **Select** for the application for which you want to schedule a backup.
 - d. In the **Recurrence** field, specify whether you want to schedule a daily or a weekly backup.
 - e. To schedule a weekly backup, select a day to run the backup from the **Day** drop-down list.
 - f. From the **Hour** drop-down list, select an hour to run the backup.
 - g. From the **Minute** drop-down list, select a minute to run the backup.
 - h. To schedule a daily backup, from the **Interval** drop-down list, specify whether the backup occurs every 6, 12, or 24 hours.

- i. Click **Submit**.



NOTE:

For a Master UIS, the default setting is a daily backup performed at 3 p.m.

For redundant applications, the active application is indicated by adding **_active** to the name.

Result:

You return to the **Scheduled Backups** page. The scheduled backup task that you created appears in the list of scheduled backups.

If any of the scheduled backup tasks fails, a trap is sent to the Unified Event Manager (UEM) application in the Lowest Zone Octet.

Postrequisites: To check that the scheduled backup file was created, go to the **Backup** page, click **Show** for the application in question, and then view the details for the backup action. In the **Results** table on the details page, you can see a time stamp for the performed backup sub-tasks. If the scheduled backup task was configured to run at 10:00 every Monday, you should find a row with this time stamp in the **Results** table.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise the scheduled backup task for the application continues to run.

4.10.5

Downloading Backup Files

Perform this procedure to download files from the zone or Master UIS to the NM Client PC.



IMPORTANT: If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.



NOTE: Only the most recent restoration point is saved in the local and central storages.

Prerequisites:

Launch the Upgrade Console application on the NM Client PC.

Log on with the **Backup** user role.

Procedure:

1. From the menu at the left, select **Download Files**.



IMPORTANT: The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for downloading. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant file.



NOTE: You can only download one file at a time.

3. In the confirmation dialog box, click **Save**.

4. In the **Save As** window, select a location and click **Save**.

Related Links

[UIS – Software Application Restoration](#) on page 93

Chapter 5

Zone Controller (ZC) Restoration

The following table lists the backup and restoration procedures of the Zone Controller (ZC) application server.

Table 10: ZC - Restoration References

Action	Reference	Done
Software restoration	ZC – Restoration Impact on page 108	
	ZC – Pre-Restoration Checks on page 109	
	ZC – Restoring Software on page 112	
	ZC – Restoring Data from Backup on page 114	
	ZC – Installing and Configuring RSA Authentication Software on page 118	
	ZC – Post-Restoration Checks on page 118	
	ZC – Backing Up Data on page 122	

5.1

ZC – Restoration Impact

Table 11: ZC – Restoration Impact

Action	Service Affected	Service Downtime
Software restoration	<p>Standby-Active switchover affects:</p> <ul style="list-style-type: none"> ● Voice communications - all sites go into Site Trunking ● Packet Data ● Short Data ● SAC download causes ZC to go Re-Loading - Radio capabilities profiles depend upon the configuration of the Default Radio and Talkgroup users and capabilities. Can affect Short Data, Packet Data, and Telephony 	<ul style="list-style-type: none"> ● All services affected only for the duration of Standby-Active switchover: approximately 5 minutes. ● Loss of ZC redundancy: approximately 5 minutes.

Related Links

[Zone Controller \(ZC\) Restoration on page 108](#)

5.2

ZC – Pre-Restoration Checks

Table 12: ZC – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	<p>Use the System Health Application Suite to check if all sites are in wide area trunking (marked with green in the grid display). Make a note if any sites are not in wide area trunking.</p> <p>Check the ZC operational status. See ZC – Checking Operational Status on page 109.</p>

5.2.1

ZC – Checking Operational Status

5.2.1.1

ZC – Viewing Zone Controller System Status

The Check System Status function checks the status, operating mode, and requested status of the Zone Controller. It also checks the status of the Zone Database Server (ZDS). Always check the operational status of the standby Zone Controller before switching it to Active. Follow the steps below to view the Zone Controller system status.

Procedure:

1. Start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**
where **<Z0>** is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223**
where **<Z0>** is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.

7. At the prompt, enter the administrator logon.
8. At the prompt, enter the password.
9. Select the option associated with the Core Server (Primary or Secondary) where the Zone Controller is located.
10. At the logon prompt, enter: sysadmin

 **NOTE:** If you are at the iLO logon prompt, enter the iLO logon and password, and then enter: exit to access the server's console.

11. At the prompt, enter the current password.

12. In the **System Administrator Main Menu**, enter the number for **Application Servers Status Administration**.

The Application Servers Status Administration list appears.

```
Application Servers Status Administration
----- 1. Enable Application Servers 2. Disable
Application Servers 3. Display Status of Application Servers 4. Application
Servers Admin and Status Commands Please enter selection (1-4, q) [q]:
```

13. Enter the number for **Display Status of Application Servers**.

 **NOTE:** The list of available application servers varies depending on the Core Server type.

The **Display Status of Application Servers** list appears.

14. Enter the number for **Zone Controller**.

Messages like the following appear:

```
The Zone Controller status is: ENABLED_ACTIVE. The Database Server status is:
ENABLED. The Zone Controller operating mode is: INTEGRATED. The Zone Controller
requested status is ENABLE.
```

 **NOTE:** See one of the following sections for descriptions of the status messages.

- [ZC – Status Descriptions on page 110](#)
- [ZC – Zone Database Server Status Descriptions on page 112](#)
- [ZC – Operating Mode Descriptions on page 112](#)
- [ZC – Requested Status Descriptions on page 112](#)

Related Links

[Zone Controller \(ZC\) Restoration](#) on page 108

5.2.1.1.1

ZC – Status Descriptions

Table 13: Zone Controller Status Descriptions

Status	Definition
ENABLED_ACTIVE	The active Zone Controller is running and has been loaded by the database server.
ENABLED_IDLE	The standby Zone Controller is running and has been loaded by the database server.

Status	Definition
STANDALONE_ACTIVE	The active Zone Controller is running, has not been loaded by the database server, and is operating off the local database because it is not connected to the ZDS.
STANDALONE_IDLE	The standby Zone Controller is running, has not been loaded by the database server, and is operating off the local database because it is not connected to the ZDS.
REMAPPING_ACTIVE	The active Zone Controller is running and reception of mapping tables from the database server is not yet complete. System is running with default subscriber access = yes.
REMAPPING_IDLE	The standby Zone Controller is running and reception of mapping tables from the database server is not yet complete. System is running with default subscriber access = yes.
LOADING_ACTIVE	The active Zone Controller is running and receiving mapping tables, subscriber records, and other data from the database server.
LOADING_IDLE	The standby Zone Controller is running and receiving mapping tables, subscriber records, and other data from the database server.
UNKNOWN	Zone Controller is unreachable.
ENABLING_ZC	Zone Controller is coming up. This is a transition state that normally is not seen.
DISABLING_ZC	Zone Controller is going down. This is a transition state that normally is not seen.
UNCONFIGURED	Initial state upon start-up.
SYNCHRONIZED WITH AUC	The Active Zone Controller has been synchronized with the Authentication Centre.
NOT SYNCHRONIZED WITH AUC	The Active Zone Controller has not been synchronized with the Authentication Centre.
SYNCHRONIZED WITH ACTIVE ZC	The Standby Zone Controller has been synchronized with the Active Zone Controller.
NOT SYNCHRONIZED WITH ACTIVE ZC	The Standby Zone Controller has not been synchronized with the Active Zone Controller.

In some of the Zone Controller statuses, an indication of ACTIVE or IDLE appears.

- ACTIVE - indicates that the Zone Controller is talking to the sites.
- IDLE - indicates that the Zone Controller is not talking to the sites.

In some of the Zone Controller statuses, an indication of ENABLE or DISABLE appears.

- ENABLE - The zone database server requests the ZC to start running.
- DISABLE - The zone database server requests the ZC to stop running.

5.2.1.1.2

ZC – Zone Database Server Status Descriptions

Table 14: ZC – Zone Database Server Statuses

Status	Definition
ENABLED	Zone database server is up.
DISABLED	Zone database server is down.
ENABLING	Zone database server is coming up.
DISABLING	Zone database server is going down.
UNKNOWN	Zone database server is unreachable.
UNCONFIGURED	Initial state upon start-up. This is a transition state that normally is not seen.

5.2.1.1.3

ZC – Operating Mode Descriptions

Table 15: ZC – Zone Controller Operating Mode Descriptions

Mode	Definition
STANDALONE	Zone database server is not communicating with the Zone Controller.
INTEGRATED	Zone database server is communicating with the Zone Controller.

 **NOTE:** If the Zone Controller status is UNKNOWN or UNCONFIGURED, the Zone Controller operating mode is not displayed.

5.2.1.1.4

ZC – Requested Status Descriptions

Table 16: ZC – Zone Controller Requested Status Descriptions

Mode	Definition
ENABLE	Indicates that the ZDS Manager has requested the Zone Controller to be Enabled.
DISABLED	Indicates that the ZDS Manager has requested the Zone Controller to be Disabled.
UNKNOWN	Indicates that the application has returned an illegal value.

5.3

ZC – Restoring Software

5.3.1

ZC – Restoring Application

Procedure:

1. On the NM Client PC, start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the Options controlling SSH key exchange pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter: 10.<Z0>.233.222

where <Z0> is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is 10.<Z0>.233.223

where <Z0> is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: `motorola`
8. At the prompt, enter the password.
9. Enter the number for the Core Server to which you want to log on.
10. At the logon prompt, enter: `instadm`
11. At the prompt, enter the current password.
The **Installation Administrator Main Menu** appears.
12. Enter the number for **Reinstall Applications**,
The list of available applications residing on the server appears.
13. Enter: `y` when the installer asks about reinstalling Zone Controller, and enter: `n` for the other applications.
The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.
14. Enter: `q` to log off the server.
15. Log on to the server by using the `sysadmin` login and password.
The **System Administrator Main Menu** appears.
16. Enter the number for **Application Servers Boot/Reboot/Shutdown**.
The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

17. Enter the number for Boot Application Servers.

The **Boot Application** menu appears.

18. Enter the number for Zone Controller.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

19. Enter: q repeatedly until you log off the server.

5.3.2

ZC – Application Configuration

No additional configuration tasks are needed once the application is restored and enabled for operation.



NOTE: Continue with the next item from [Table 10: ZC - Restoration References on page 108](#).

Related Links

[Zone Controller \(ZC\) Restoration](#) on page 108

5.4

ZC – Restoring Data from Backup

5.4.1

ZC – Logging On to the Server

Prerequisites: Ensure that the server is on.

Procedure:

1. Start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**
where **<Z0>** is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223**

where **<Z0>** is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the PuTTY Security Alert window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: `motorola`
8. At the prompt, enter the password.
9. Enter the number for the server you want to log on to.
10. At the logon prompt, enter: `sysadmin`
11. At the prompt, enter the current password.
The **System Administrator Main Menu** appears.
12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.

5.4.2

ZC – Disabling the Application Server

Prerequisites: Before you start this procedure, you must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the Zone Controller application server.
A message appears showing that the application server is disabled.
4. Enter: `q` twice to go back to the **Application Servers Status Administration** menu.

5.4.3

ZC – Restoring Data from Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. Select **Restore** in the menu at the left side of the Upgrade Console.
A table appears showing available backup files for applications in the different zones.
2. Click **Refresh filename**.
The file names of the backup files are read on the default storage for each application. If you configured the usage of central storage for the backup, the default storage is Master UIS. Otherwise, it is Zone UIS. If you configured a Storage PC then a list of backup file names stored on Storage PCs will be available.

3. Select **Backup Filename** and from the drop-down list, choose the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named `zone<XX>_zcdb_01_<timestamp>.tar.gz` or `zone<XX>_zcdb_02_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.



NOTE: You can only download one file at a time.

A warning appears asking whether you want to save the file.

5. Click **Yes**.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has completed.

5.4.4

ZC – Enabling the Application Server

Prerequisites: Before you start this procedure, you must be logged in to the server, and the **System Administrator Main Menu** menu must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Enable All Application Servers**.
3. Enter the number associated with the Zone Controller application server.

A message appears showing that the application server is enabled.

Related Links

[Zone Controller \(ZC\) Restoration](#) on page 108

5.5

Displaying Current KVL Assignment

Perform this procedure to check the current serial port assignment for Key Variable Loader (KVL) communication.

Prerequisites: Log on as `instadm` using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server](#) on page 45
- [Logging On to iGAS Through a KVM Switch](#) on page 48

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **Application Device Management**.

The **Application Device Management** appears:

Application Device Management

- 1. Display current device assignment
- 2. Attach device to Application

Please enter selection (1-2, q) [q]:

3. Enter the number for **Display current device assignment**.

The current port assignment appears.

5.6

Attaching KVL to Application

Perform this procedure to configure serial port 2 assignment for Key Variable Loader (KVL) communication if you are restoring a Core Server in the Primary Zone.

Prerequisites: Log on as `instadm` using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:

2. Enter the number for **Application Device Management**.

The **Application Device Management** menu appears:

Application Device Management

- 1. Display current device assignment
- 2. Attach device to Application

Please enter selection (1-2, q) [q]:

3. Enter the number for **Attach device to Application**.

The **Attach device to Application** menu appears.

4. Enter the number for the application to which you want to attach serial port 2 for KVL communication.

The port assignment is changed and the **Application Device Management** menu appears.

5. To verify the current iGAS devices configuration, enter the number for **Display current device assignment**.

6. Optional: For systems with Air Interface Encryption (AIE): perform Reprovisioning Zone Entity with an Existing Infrastructure Key in the *Authentication Centre (AuC) User Manual*.

5.7

ZC – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.



IMPORTANT: When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[Zone Controller \(ZC\) Restoration](#) on page 108

5.8

ZC – Post-Restoration Checks

Table 17: ZC – Post-Restoration Checks

Action	Post-Restoration Checks
Zone Controller software restoration – Standby ZC	<p>Check system status from ZC admin menus. See ZC – Checking Operational Status on page 109.</p> <p>Check the ZC redundancy status.</p> <p>Test all call types (if possible).</p>
Zone Controller software restoration – Test once the Standby ZC is made Active	<p>Use System Health Application Suite to test how many sites are wide area.</p> <p>Security Class Operation (check if there are keys used in a call from System Health Application Suite).</p> <p>Nationwide operation (Multi-Cluster voice and data).</p>

5.8.1

ZC – Checking Operational Status

5.8.1.1

ZC – Viewing Zone Controller System Status

The Check System Status function checks the status, operating mode, and requested status of the Zone Controller. It also checks the status of the Zone Database Server (ZDS). Always check the operational status

of the standby Zone Controller before switching it to Active. Follow the steps below to view the Zone Controller system status.

Procedure:

1. Start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the Options controlling SSH key exchange pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**

where <Z0> is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223**

where <Z0> is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the prompt, enter the administrator logon.
8. At the prompt, enter the password.
9. Select the option associated with the Core Server (Primary or Secondary) where the Zone Controller is located.
10. At the logon prompt, enter: sysadmin



NOTE: If you are at the iLO logon prompt, enter the iLO logon and password, and then enter: **exit** to access the server's console.

11. At the prompt, enter the current password.

12. In the **System Administrator Main Menu**, enter the number for **Application Servers Status Administration**.

The Application Servers Status Administration list appears.

```
Application Servers Status Administration
----- 1. Enable Application Servers 2. Disable
Application Servers 3. Display Status of Application Servers 4. Application
Servers Admin and Status Commands Please enter selection (1-4, q) [q]:
```

13. Enter the number for **Display Status of Application Servers**.



NOTE: The list of available application servers varies depending on the Core Server type.

The **Display Status of Application Servers** list appears.

14. Enter the number for **Zone Controller**.

Messages like the following appear:

The Zone Controller status is: ENABLED_ACTIVE. The Database Server status is: ENABLED. The Zone Controller operating mode is: INTEGRATED. The Zone Controller requested status is ENABLE.



NOTE: See one of the following sections for descriptions of the status messages.

- [ZC – Status Descriptions on page 120](#)
- [ZC – Zone Database Server Status Descriptions on page 121](#)
- [ZC – Operating Mode Descriptions on page 121](#)
- [ZC – Requested Status Descriptions on page 122](#)

Related Links

[Zone Controller \(ZC\) Restoration](#) on page 108

5.8.1.1

ZC – Status Descriptions

Table 18: Zone Controller Status Descriptions

Status	Definition
ENABLED_ACTIVE	The active Zone Controller is running and has been loaded by the database server.
ENABLED_IDLE	The standby Zone Controller is running and has been loaded by the database server.
STANDALONE_ACTIVE	The active Zone Controller is running, has not been loaded by the database server, and is operating off the local database because it is not connected to the ZDS.
STANDALONE_IDLE	The standby Zone Controller is running, has not been loaded by the database server, and is operating off the local database because it is not connected to the ZDS.
REMAPPING_ACTIVE	The active Zone Controller is running and reception of mapping tables from the database server is not yet complete. System is running with default subscriber access = yes.
REMAPPING_IDLE	The standby Zone Controller is running and reception of mapping tables from the database server is not yet complete. System is running with default subscriber access = yes.
LOADING_ACTIVE	The active Zone Controller is running and receiving mapping tables, subscriber records, and other data from the database server.
LOADING_IDLE	The standby Zone Controller is running and receiving mapping tables, subscriber records, and other data from the database server.
UNKNOWN	Zone Controller is unreachable.
ENABLING_ZC	Zone Controller is coming up. This is a transition state that normally is not seen.
DISABLING_ZC	Zone Controller is going down. This is a transition state that normally is not seen.
UNCONFIGURED	Initial state upon start-up.

Status	Definition
SYNCHRONIZED WITH AUC	The Active Zone Controller has been synchronized with the Authentication Centre.
NOT SYNCHRONIZED WITH AUC	The Active Zone Controller has not been synchronized with the Authentication Centre.
SYNCHRONIZED WITH ACTIVE ZC	The Standby Zone Controller has been synchronized with the Active Zone Controller.
NOT SYNCHRONIZED WITH ACTIVE ZC	The Standby Zone Controller has not been synchronized with the Active Zone Controller.

In some of the Zone Controller statuses, an indication of ACTIVE or IDLE appears.

- ACTIVE - indicates that the Zone Controller is talking to the sites.
- IDLE - indicates that the Zone Controller is not talking to the sites.

In some of the Zone Controller statuses, an indication of ENABLE or DISABLE appears.

- ENABLE - The zone database server requests the ZC to start running.
- DISABLE - The zone database server requests the ZC to stop running.

5.8.1.1.2

ZC – Zone Database Server Status Descriptions

Table 19: ZC – Zone Database Server Statuses

Status	Definition
ENABLED	Zone database server is up.
DISABLED	Zone database server is down.
ENABLING	Zone database server is coming up.
DISABLING	Zone database server is going down.
UNKNOWN	Zone database server is unreachable.
UNCONFIGURED	Initial state upon start-up. This is a transition state that normally is not seen.

5.8.1.1.3

ZC – Operating Mode Descriptions

Table 20: ZC – Zone Controller Operating Mode Descriptions

Mode	Definition
STANDALONE	Zone database server is not communicating with the Zone Controller.
INTEGRATED	Zone database server is communicating with the Zone Controller.



NOTE: If the Zone Controller status is UNKNOWN or UNCONFIGURED, the Zone Controller operating mode is not displayed.

5.8.1.1.4

ZC – Requested Status Descriptions

Table 21: ZC – Zone Controller Requested Status Descriptions

Mode	Definition
ENABLE	Indicates that the ZDS Manager has requested the Zone Controller to be Enabled.
DISABLED	Indicates that the ZDS Manager has requested the Zone Controller to be Disabled.
UNKNOWN	Indicates that the application has returned an illegal value.

5.9

ZC – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

5.9.1

ZC – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

5.9.2

ZC – Configuring a Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **zc01** or **zc02** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the ZC application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **zc01** or **zc02** application in the **Use Central Storage** column. Make sure that you select the check box for the ZC in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **zc01** or **zc02** application in the **Use Storage PC** column.

 **NOTE:** It will be saved on all Storage PCs.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [ZC – Backing Up Data On-Demand on page 123](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [ZC – Scheduling Backup on page 124](#).
- You can do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise the scheduled backup task for the application continues to run.

5.9.3

ZC – Backing Up Data On-Demand

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **zc01** or **zc02** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites: You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [ZC – Scheduling Backup on page 124](#).
- If you want to save the backup file on the NM Client PC, continue to [ZC – Downloading a Backup File to the NM Client PC on page 125](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

5.9.4

ZC – Scheduling Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Perform the following actions:
 - a. In the **Name** field, type a name for the scheduled backup task.
 - b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.
A list appears in which you must click **Select** in the row containing the **zc01** or **zc02** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.
 - c. In the **Day** drop-down list, select a week day or select **DAILY**.
 - d. In the **Hour** drop-down list, select at which hour the backup must run.
 - e. In the **Minute** drop-down list, select at which minute the backup must run.
 - f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.
4. If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [ZC – Downloading a Backup File to the NM Client PC on page 125](#). Otherwise, you do not have to do anything more regarding backup.

Postrequisites:

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

5.9.5

ZC – Downloading a Backup File to the NM Client PC



NOTE: If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Prerequisites:



IMPORTANT: If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.



IMPORTANT: The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.



NOTE:
The backup file is named `zone<XX>_zcdb_01_<timestamp>.tar.gz` or `zone<XX>_zcdb_02_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

You can only download one file at a time.

A warning appears asking whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[Zone Controller \(ZC\) Restoration](#) on page 108

Chapter 6

Air Traffic Router (ATR) – Software Application Restoration

Table 22: ATR – Restoration References

Action	Reference	Done
Software restoration	ATR – Restoration Impact on page 126	
	ATR – Restoring Application on page 126	
	ATR – Configuring Application on page 127	
	ATR – Restoring Data from Backup on page 129	
	ATR – Installing and Configuring RSA Authentication Software on page 131	
	ATR – Post-Restoration Checks on page 131	
	ATR – Backing Up Data on page 131	

6.1

ATR – Restoration Impact

Table 23: ATR – Restoration Impact

Action	Service Affected	Service Downtime
Software restoration	<ul style="list-style-type: none"> RCM including CADI/Multi-CADI ATIA including voice recording and billing Historical Reports System Health Application Suite DSSA 	<ul style="list-style-type: none"> All services affected only for the duration of Standby-Active switchover: approximately 2 minutes. Loss of ATR redundancy: approximately 5 minutes.

6.2

ATR – Restoring Software

6.2.1

ATR – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)

- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to re-install Air Traffic Router, and enter: `n` for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering `q`

5. Log on to iGAS as `sysadmin`

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number associated with Air Traffic Router.

You have booted the application.

9. Enter: `q` and repeat this sequence until you log off from the server.

Related Links

[Air Traffic Router \(ATR\) – Software Application Restoration on page 126](#)

6.2.2

ATR – Configuring Application

The following describes how to properly configure the Air Traffic Router (ATR) application server.

6.2.2.1

ATR – Enabling the Application Server

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.



NOTE: The list of available servers varies depending on the deployment type.

The list of servers appears.

3. Enter the number associated with the ATR application server.

The login prompt appears.

4. Log in as **atradmin**.



NOTE: The initial administrative prompts vary depending on the application server in question.

The application server displays initial administrative prompts.

5. Confirming by pressing **ENTER**, answer the application server's initial prompts.

You are logged on, and the Main Menu appears.

```
Air Traffic Router Administration 1. Enable ATR Server 2. Disable ATR Server 3.
Display Server Status 4. Server Administration 5. ATIA Call Logging Parameter
Setup 6. ATIA Stream IP Address Configuration 7. Routes Configuration 8. CADI
Fault Management Setup 9. Database Administration 10. Backup Administration 11.
RCM Legacy Interface Setup Enter Selection: (1-11, q, ?) [q]>
```

6. Enter the number associated with **Enable ATR Server**.

Process messages appear that indicate the application server has been enabled, followed by the application servers Administration menu.

6.3

ATR – Restoring Data from Backup

Prerequisites: You must be logged on to the ESU on the Master UIS, with the Backup user role. A data backup file must be available. The application server that you want to restore must be enabled. If the application server is disabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named `zone<XX>_atrb_01_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

6.4

UCS – Collect and Combine

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

System Administrator Main Menu

1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown

```
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

The **Application Servers Administration Menus** appear.



NOTE: The list of available servers varies depending on the deployment type.

3. Enter the number associated with the UCS application server.

The login prompt appears.

4. Log in as ucadmin.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Confirm by pressing **ENTER** and answer the application server's initial prompts.

You are logged on, and the **User Configuration Server Administration** appears.

```
User Configuration Server Administration 1. Enable User Configuration Server 2.
Enable User Configuration Server (fast) 3. Disable User Configuration Server 4.
Display Server Status 5. Database Administration 6. Feature Administration 7.
Unix Administration 8. Backup Server Administration 9. Multicloud Radio Control
Manager Administration 10. UCS Report Administration Enter Selection: (1-10, q, ?)
[q]>
```



IMPORTANT: In multicloud systems that include servers which do not support security mode, you need to perform [step 6](#) through [step 9](#) to disable security mode on all servers. This ensures the collect and combine operation success. In other scenarios, you can go to [step 10](#).

6. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

7. Enter the number for **Toggle security mode**.

8. At the prompt to confirm disabling the security mode, enter: Y

9. Return to the **User Configuration Server Administration** menu.

10. Enter the number associated with **Multicloud Radio Control Manager Administration**.

The **Multicloud Radio Control Manager Administration** menu appears:

```
Multicloud Radio Control Manager Administration 1. Export Radio Control Manager
Data 2. Collect and Combine Radio Control Manager Data 3. Configure Automatic
Radio Control Manager Export 4. Configure Automatic Collect and Combine of Radio
Control Manager Export 5. Enable Automatic Export, Collect and Combine of Radio
Control Manager Data 6. Disable Automatic Export, Collect and Combine of Radio
Control Manager Data 7. Display Status of Radio Control Manager Operations 8.
Display History of Radio Control Manager Operations Enter Selection: (1-8,,q, ?):
```

11. Enter the number associated with **Collect and Combine Radio Control Manager Data**.

The following exemplary message indicates that the action is complete:

```
2016-07-26 19:12:07| Transfer and merge of Multicloud RCM data completed
successfully... 2016-07-26 19:12:08| Data distribution to the ATR servers is in
progress. You can check its status from the menu.
```

12. Return to the Server Administration menu by entering q

Related Links

[Air Traffic Router \(ATR\) – Software Application Restoration](#) on page 126

6.5

ATR – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[Air Traffic Router \(ATR\) – Software Application Restoration](#) on page 126

6.6

ATR – Post-Restoration Checks

Table 24: ATR – Post-Restoration Checks

Action	Post-Restoration Checks
Software restoration	<p>Check that CADI/RCM is operational.</p> <p>Check that Multi-CADI is operational.</p> <p>Check System Health Application Suite and Historical Reports.</p> <p>Ensure ATIA is now being received at the required Host/Hosts with end-user confirmation.</p>

6.7

ATR – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

6.7.1

ATR – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

6.7.2

ATR – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console. A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **atr01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the ATR application in the correct zone.
 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.
3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **atr01** application in the **Use Central Storage** column. Make sure that you select the check box for the ATR in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **atr01** application in the **Use Storage PC** column.
 **NOTE:** The backup file is cumulatively added to the backups on the Storage PC.
5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [ATR – Backing Up Data On-Demand on page 133](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [ATR – Scheduling Backup on page 133](#).
- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

6.7.3

ATR – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **atr01** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The Backup Status column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [ATR – Scheduling Backup on page 133](#).
- If you want to save the backup file on the NM Client PC, continue to [ATR – Downloading a Backup File to the NM Client PC on page 134](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

6.7.4

ATR – Scheduling Backup

Prerequisites: Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Perform the following actions:
 - a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **atr01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.
- d. In the **Hour** drop-down list, select at which hour the backup must run.
- e. In the **Minute** drop-down list, select at which minute the backup must run.
- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [ATR – Downloading a Backup File to the NM Client PC on page 134](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

6.7.5

ATR – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `zone<XX>_atrdb_01_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[Air Traffic Router \(ATR\) – Software Application Restoration](#) on page 126

Chapter 7

Alias Server – Software Application Restoration

Table 25: Alias Server – Restoration Reference

Action	Reference	Done
Software Restoration	AS – Restoration Impact on page 136	
	AS – Pre-Restoration Checks on page 136	
	AS – Restoring Software on page 137	
	AS – Configuring Application (Windows Server 2016 Procedures) on page 138	
	AS – Installing and Configuring RSA Authentication Software on page 142	
	AS – Post-Restoration Checks on page 142	
	AS – Backing Up Data on page 143	

7.1

AS – Restoration Impact

Table 26: Alias Server – Restoration Impact

Action	Service Affected	Service Downtime
Software Restoration	<ul style="list-style-type: none"> RUA/RUI service dimmed out A new radio will fail to log in (logged radios will not be impacted) 	All services affected for approximately 5 minutes.

7.2

AS – Pre-Restoration Checks

 **IMPORTANT:** Before starting the restoration procedures, check for any new Motorola Solutions Technical Notification (MTN).

Table 27: AS – Restoration Prerequisites

Type	Description
	Alias Server application
Software	Alias Provisioning Client application
	Alias SNMP Agent

Type	Description
	PostgreSQL

7.3

AS – Restoring Software

7.3.1

AS – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Type the number associated with **Reinstall Applications** and press **Enter**.
The list of available applications residing on the server appears.
3. Enter **y** when the installer asks about reinstalling Alias Server, and type **n** for other applications.
The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.
4. Enter: **q** to log off the server.
5. Log on to iGAS as `sysadmin`

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Type the number associated with **Application Servers Boot/Reboot/Shutdown** and press **Enter**.
The **Application Servers Boot/Reboot/Shutdown** menu appears.
7. Type the number associated with **Boot Application Servers** and press **Enter**.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

8. Type the number associated with Alias Server and press **Enter**.

You have booted the application.

9. Enter: **q** repeatedly until you log off the server.

Related Links

[Alias Server – Software Application Restoration](#) on page 136

7.3.2

AS – Configuring Application (Windows Server 2016 Procedures)

The following section covers configuring Alias Server based on the Windows Server 2016 architecture.

7.3.2.1

AS – Installing Distinct ONC RPC License

 **IMPORTANT:** The Distinct ONC RPC software is installed automatically, but ensure that you have obtained the license. A serial number and a key code are required to successfully complete the installation of Distinct ONC RPC software.

Procedure:

1. Run the command line interface as an administrator.
2. Navigate to the following directory: **%AS_HOME%** (`cd %AS_HOME%`)
3. Run the following script with the following two parameters:
`register_distinct.bat <SerialNumber> <KeyCode>`

Step example:

`register_distinct.bat A1234567890123456 A0-B1-C2`

Postrequisites: Restart the application server.

7.3.2.2

Rebooting the Alias Server

Procedure:

1. Log in to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Type the number associated with **Application Servers Boot/Reboot/Shutdown** and press **Enter**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown
-----
1. Boot Application Servers
2. Reboot Application Servers
3. Shutdown Application Servers
Please enter selection (1-3, q) [q] :
```

3. Type the number associated with **Reboot Application Servers** and press **Enter**.
The **Boot Application** menu appears.
4. Type the number associated with **Alias Server** and press **Enter**.
The Alias Server application residing on the server reboots.

Related Links

[Alias Server – Software Application Restoration](#) on page 136

7.4

AS – Restoring Data from Backup

7.4.1

AS – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [AS – Uploading a Backup File to UIS on page 139](#). If the backup file already is in the UIS backup storage, continue to [Accessing Virtual Machines with the Web-Based Client on page 140](#).

7.4.2

AS – Uploading a Backup File to UIS

Prerequisites: Log on to the Upgrade Console with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the Upgrade Console.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.

 **NOTE:** If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Upload Files**.

The **Upload Files** screen appears.

2. Click **Browse**.

3. In the window that appears, select your backup file. Click **OK**.

 **NOTE:** The backup file is named `cluster<XX>_asdb_<YY>_<timestamp>`, where `<XX>` is the cluster ID, `<YY>` is the alias ID and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

5. Click **Analyze Uploaded File**.

If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

7.4.3

Accessing Virtual Machines with the Web-Based Client

Procedure:

1. Open a web browser (Chromium).

2. In the address field, enter the IP address of the HostOS you want to access.

3. Perform the following actions:

- a. In the **User name** field, enter: sysadmin
- b. In the **Password** field, enter the password.
- c. Click **Log in**.

4. In the Web-based client, perform the following actions:

- a. In the **Navigator** pane, click **Virtual Machines**.

 **NOTE:** If a red exclamation mark is visible next to **System Time information** under the **System** tab in the **Navigator**, you can ignore it. To verify system time synchronization status, you can log in to IGAS as sysadmin user and use the NTP Administration menu.

- b. On the **Virtual Machines** list, select the check box next to the Virtual Machine you want to access.

- c. Select the **Consoles** tab.

- d. In the **Console Type** section, select **VNC**.

 **IMPORTANT:** Do not use other console types.

The graphical console appears in a new window.

 **NOTE:** If a VNC connection to virtual machine in Cockpit fails to pass keystrokes, you can press **CTRL+ALT+DEL**, and fold and unfold the virtual machine bar.

 **NOTE:** After a fresh installation or upgrade of CCE on DCS server, an unexpected Microsoft Windows dialog box appears, prompting you to restart your computer to apply the changes. You can ignore it or click **Restart Later**.

7.4.4

AS – Restoring Data from Backup

Prerequisites:

You must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be enabled. If the application server is disabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup zip file is named **zoneXX_asdb_01_timestamp**, where XX is the zone ID, and timestamp is a date and time written as one row of digits with the format **yyyymmddhhmm**.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

7.4.5

AS – Enabling the Application Server

You can perform this procedure to enable the Alias Server (AS) application server before restoring the application. If the application server is disabled, the restoration fails.

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
```

```
-----
```

1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown

```
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

7.5

AS – Installing and Configuring RSA Authentication Software

Procedure:

1. Clear 2FA Secret key on the RSA server. See the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.



IMPORTANT:

When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

The RSA Agent installation should be performed after the promoting of Domain Controller.

Related Links

[Alias Server – Software Application Restoration](#) on page 136

7.6

AS – Post-Restoration Checks

Table 28: AS – Post-Restoration Checks

Action	Post-Restoration Checks
All restoration procedures	<p>Check whether the AS can connect to the MultiCADI and the ZC. See AS – Checking the AS Application on page 142 for details.</p>
	<p>Check whether the Alias Provisioning Client can start successfully on the active Alias Server instance.</p>

7.6.1

AS – Checking the AS Application

Double-click on the Alias Server icon on the Desktop. The **Alias Server** window is displayed. Make sure the application is connected to the CADI Server and the configuration files are loaded successfully. Check whether UEM receives the SNMP traps from the Alias Server or not. If problems are encountered, see the troubleshooting section in the *Call Processing and Mobility Management* manual for possible solutions.

Related Links

[Alias Server – Software Application Restoration](#) on page 136

7.7

AS – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

7.7.1

AS – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

7.7.2

AS – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **alias_active** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the AS application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [AS – Backing Up Data On-Demand on page 144](#).

- If you want to create a scheduled backup task running at regular intervals, continue to [AS – Scheduling Backup on page 144](#).
- You can do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

7.7.3

AS – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **alias_active** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [AS – Scheduling Backup on page 144](#).
- If you want to save the backup file on the NM Client PC, continue to [AS – Downloading a Backup File to the NM Client PC on page 145](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

7.7.4

AS – Scheduling Backup

Prerequisites: Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

a. In the **Name** field, type a name for the scheduled backup task.

b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **alias_active** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

c. In the **Day** drop-down list, select a week day or select **DAILY**.

d. In the **Hour** drop-down list, select at which hour the backup must run.

e. In the **Minute** drop-down list, select at which minute the backup must run.

f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [AS – Downloading a Backup File to the NM Client PC on page 145](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

7.7.5

AS – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Save**.

3. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[Alias Server – Software Application Restoration](#) on page 136

Chapter 8

MultiCADI – Software Application Restoration

Table 29: MultiCADI – Restoration References

Action	Reference	Done
Software Restoration with backup available	MultiCADI – Restoring Application on page 146 MCADI – Restoring Data from Backup on page 148 MCADI – Installing and Configuring RSA Authentication Software on page 151 MultiCADI – Post-Restoration Checks on page 151 MultiCADI – Backing Up Data on page 153	
Full Software Restoration without any backup stored	MultiCADI – Restoring Application on page 146 MultiCADI – Installing Software Components on page 148 MultiCADI – Application Configuration on page 148 MCADI – Installing and Configuring RSA Authentication Software on page 151 MultiCADI – Post-Restoration Checks on page 151 MultiCADI – Backing Up Data on page 153	

8.1

MultiCADI – Restoring Software

 **IMPORTANT:** Before starting the restoration procedures, check for any new Motorola Solutions Technical Notification (MTN).

8.1.1

MultiCADI – Restoring Application

Prerequisites: Log on to the server as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

Installation Administrator Main Menu 1. Reinstall Applications 2. View Installation Information 3. View Installation Log 4. License Administration 5. Load software from DVD 6. Application DVD Management

```
7. Application Device Management 8. Change password 9. Security Update Services  
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: **y** when the installer prompts you to re-install MultiCADI and enter: **n** for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering **q**
5. Log on to the server using the **sysadmin** login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu  
-----  
1. Enable all Application Servers  
2. Disable all Application Servers  
3. Display Status of all Application Servers  
4. Unix Administration  
5. Application Servers Administration Menus  
6. Application Servers Boot/Reboot/Shutdown  
7. Application Servers Status Administration  
8. Application Isolation Management  
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown  
-----  
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application  
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number associated with MultiCADI.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.



NOTE: After a reboot, if MultiCADI reports **enabled** state, but MultiCADI GUI Client does not report CADI Server as **Logged In**, reboot the machine again. For details, see "MultiCADI GUI Client Startup" in the *MultiCADI* manual.

9. Enter: **q** and repeat this sequence until you log off from the server.

Postrequisites: If you have a backup, perform steps in [MCADI – Restoring Data from Backup on page 148](#). If you do **not** have a backup, perform steps in "MultiCADI - Software Installation and Configuration" in the *MultiCADI* manual.

Related Links

[MultiCADI – Software Application Restoration](#) on page 146

8.2

MultiCADI – Application Configuration

For more information on MultiCADI configuration, see "MultiCADI - Software Installation and Configuration" in the *MultiCADI* manual.

8.3

MCADI – Restoring Data from Backup

8.3.1

MultiCADI – Installing Software Components

Prerequisites: To install the MultiCADI software components on your computer, log on to the MultiCADI server as the Administrator. The Distinct ONC RPC software is installed automatically, only provide the license serial number and key (as described in the procedure below).

 **IMPORTANT:** Ensure that you have obtained the Distinct license. A serial number and a key code are required to successfully complete the installation.

 **NOTE:** You cannot run any other Distinct applications on the MultiCADI Server when you are not logged as the System user. You will get the message: License violation.

Procedure:

1. Click **Start**.
2. Select the **MultiCADI <Rxx.xx.xx.xx>** folder, where **<Rxx.xx.xx.xx>** is the version of the application installed on your computer.
3. Open the **Distinct License Manager**.
Messages informing about the process, verifying the license and Distinct installation appear.
 **NOTE:** If the serial number and the key are entered incorrectly, you are not notified about it. The message informing about saving the license still appears. However, the MultiCADI software does not start correctly.
4. Restart the operating system.

Related Links

[MultiCADI – Software Application Restoration](#) on page 146

8.3.2

MCADI – Enabling the Application Server

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server](#) on page 45
- [Logging On to iGAS Through a KVM Switch](#) on page 48

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

Related Links

[MultiCADI – Software Application Restoration](#) on page 146

8.3.3

MCADI – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [MCADI – Uploading a Backup File to UIS on page 149](#).

8.3.4

MCADI – Uploading a Backup File to UIS

Prerequisites: Log on to the Upgrade Console with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the Upgrade Console.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.



NOTE: If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Upload Files**.

The **Upload Files** screen appears.

2. Click **Browse**.

3. In the window that appears, select your backup file. Click **OK**.

 **NOTE:** The backup file is named zone<XX>_mcadidb_01_<timestamp>, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

5. Click **Analyze Uploaded File**.

If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

8.3.5

MCADI – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named zone<XX>_mcadidb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

8.4

MultiCADI – Network Security Software Installation

 **NOTE:** The installation of the AntiVirus client is optional. For details, see the relevant section in the “Installation and Configuration” chapter of the *Network Security* manual.

8.4.1

MCADI – Installing and Configuring RSA Authentication Software

Procedure:

1. Clear 2FA Secret key on the RSA server. See the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.



IMPORTANT:

When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

The RSA Agent installation should be performed after the promoting of Domain Controller.

Related Links

[MultiCADI – Software Application Restoration](#) on page 146

8.4.2

MultiCADI – AntiVirus Client Installation

 **NOTE:** The installation of the AntiVirus client is optional. For details, see the relevant section in the “Installation and Configuration” chapter of the *Network Security* manual.

8.5

MultiCADI – Post-Restoration Checks

8.5.1

MultiCADI – Checking the Configuration Tool

Right-click **Start** and select **Search**. In the **Search** field, enter: MultiCADI Configuration Tool command. The Configuration Tool window is displayed. Ensure that no error or warning appears in the window. Otherwise, see the troubleshooting section for possible solutions.

8.5.2

MultiCADI – Enabling the MultiCADI

You enable and disable application servers from their respective administration menus. Enabling an application server starts all of the processes necessary for the server to function properly in the system.

Perform this procedure only in case of restoring software without any backup stored. If backup is available, skip this procedure.

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

The list of server status options appears.

```
1. Enable Application Servers 2. Disable Application Servers 3. Display Status of
Application Servers 4. Application Servers Admin and Status Commands Please enter
selection (1-4, q) [q]
```

3. Enter the number associated with **Enable Application Servers**.



NOTE: The list of available servers varies depending on the deployment type.

The list of servers appears.

```
1. Air Traffic Router (atr01.zone3)
2. MultiCADI Server (mcadi01.zone3)
3. Enable all applications
Please enter selection (1-4, q) [q]:
```

4. Enter the number associated with the **MultiCADI Server**.

8.5.3

MultiCADI – Checking the MultiCADI Application

Right-click **Start** and select **Search**. In the **Search** field, enter: MultiCADI GUI command. The **MultiCADI** window will be displayed. Ensure the application is connected to the CADI Server and the configuration files are loaded successfully. If you have configured the SNMP section, check whether the UEM receives the SNMP traps from MultiCADI or not (MultiCADI has to be enabled on iGAS first). If problems are encountered, see the troubleshooting section for possible solutions.

Related Links

[MultiCADI – Software Application Restoration](#) on page 146

8.6

MultiCADI – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

8.6.1

MultiCADI – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

8.6.2

MultiCADI – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.
A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **mcadi01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the MCADI application in the correct zone.
 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.
3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **mcadi01** application in the **Use Central Storage** column. Make sure that you select the check box for the MCADI in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **mcadi01** application in the **Use Storage PC** column.



NOTE: The backup file is cumulatively added to the backups on the Storage PC.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [MultiCADI – Backing Up Data On-Demand on page 154](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [MultiCADI – Scheduling Backup on page 155](#).
- You can do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

8.6.3

MultiCADI – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **mcadi01** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [MultiCADI – Scheduling Backup on page 155](#).
- If you want to save the backup file on the NM Client PC, continue to [MultiCADI – Downloading a Backup File to the NM Client PC on page 155](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

8.6.4

MultiCADI – Scheduling Backup

Prerequisites: Log on the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

- a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **mcadi01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.

- d. In the **Hour** drop-down list, select at which hour the backup must run.

- e. In the **Minute** drop-down list, select at which minute the backup must run.

- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [MultiCADI – Downloading a Backup File to the NM Client PC on page 155](#). Otherwise, you do not have to do anything else regarding backup.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

8.6.5

MultiCADI – Downloading a Backup File to the NM Client PC

Prerequisites:



IMPORTANT: If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.



NOTE: If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named zone<XX>_mcadirdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.

4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[MultiCADI – Software Application Restoration](#) on page 146

Chapter 9

Authentication Centre (AuC) Software Application Restoration

Table 30: AuC – Restoration References

Action	Reference	Done
AuC Restoration	AuC – Restoration Impact on page 157	
	AuC – Pre-Restoration Checks on page 158	
	AuC – Restoring Application on page 162	
	AuC – Restoring Data from Backup on page 165	
	AuC – Configuring Application on page 172	
	AuC – Installing and Configuring RSA Authentication Software on page 178	
	AuC – Post-Restoration Checks on page 178	
AuC Database Restoration	AuC – Restoration Impact on page 157	
	AuC – Pre-Restoration Checks on page 158	
	AuC – Restoring Data from Backup on page 165	
	AuC – Configuring Application on page 172	
	AuC – Installing and Configuring RSA Authentication Software on page 178	
	AuC – Post-Restoration Checks on page 178	
Replacing AuC CryptR2	AuC – Restoration Impact on page 157	
	AuC – Pre-Restoration Checks on page 158	
	Replacing CryptR2 on page 168	
	AuC – Post-Restoration Checks on page 178	

9.1

AuC – Restoration Impact

Table 31: AuC – Restoration Impact

Action	Service Affected	Service Downtime
AuC container restoration	<ul style="list-style-type: none"> No distribution of keys and authentication material. No updates of keys and authentication material. 	Approximately 30 minutes, depending on the size of database

Action	Service Affected	Service Downtime
AuC database restoration	<ul style="list-style-type: none"> • No distribution of keys and authentication material. • No updates of keys and authentication material. 	Approximately a couple of minutes, depending on the size of database
CryptR2 replacement	<ul style="list-style-type: none"> • No distribution of keys and authentication material. • No updates of keys and authentication material. 	Approximately 0.5 hour

Related Links

[Authentication Centre \(AuC\) Software Application Restoration](#) on page 157

9.2

AuC – Pre-Restoration Checks

Table 32: AuC – Pre-Restoration Checks

Action	Pre-Restoration Checks
All restoration procedures	<p>Back up the database (if possible).</p> <p>Check statuses of the:</p> <ul style="list-style-type: none"> UCS, ZDSs - for more information, see the <i>Network Management Servers</i> manual. ZCs - AuC – Checking Status of the Zone Controller on page 158 <p>base sites on the AuC Client, if available. Alternatively, use UEM/System Health Application Suite.</p>
	Determine Key Version Numbers in AuC Backup File.

9.2.1

AuC – Checking Status of the Zone Controller

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server](#) on page 45
- [Logging On to iGAS Through a KVM Switch](#) on page 48

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
```

8. Application Isolation Management
Please enter selection (1-8, q) [q]:

2. Enter the number associated with **Application Servers Administration Menus**.

The Application Servers Administration Menus list appears.



NOTE: The list of available application servers varies depending on the Core Server type.

3. Enter the number associated with **Zone Controller**.

The login prompt appears.

4. Log in as szadmin.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Press **ENTER** to close each application server's initial prompt.

You are logged on, and the **System Administration** menu appears.

System Administration 1. Database Administration 2. Zone Controller Administration
3. Zone Call Processing Administration 4. Unix Administration 5. Live Upgrade
Administration 6. Install Additional Software 7. Turn off/on Messages Enter
Selection: (1-7, q, ?) [q]

6. On the System Administration menu, press the number key associated with **Zone Controller Administration**, and then press **Enter**.

The **Zone Controller Administration** menu appears.

Zone Controller Administration 1. Enable Zone Controller 2. Disable Zone
Controller 3. Check System Status 4. Component States 5. Alarm States 6.
Redundancy Administration 7. Zone Controller Locator Light Enter Selection:
(1-7, q, ?) [q]

7. On the **Zone Controller Administration** menu, press the number key associated with **Check System Status**, then press **Enter**.

The System status information appears. Example messages is shown below:

The Zone Controller status is: ENABLED_ACTIVE. The Database Server status is:
ENABLED. The Zone Controller operating mode is: INTEGRATED. The Zone Controller
requested status is ENABLE.

8. Verify that the active ZC shows **Enabled_Active**.

9.2.2

AuC – Recording the Key Version Numbers

Procedure:

1. Launch the AuC client.
2. Log on as a valid user with appropriate permissions.
3. From the toolbar, select **System** → **Go Out of Service**.
The event is logged in the **Events** window.
4. Open the **Zones** tab.

5. Record the KEKm, KEKz, CCK, and SCK Present and Future Key Version Numbers for the Zone as reported on the AuC Client.

9.2.3

AuC – Determining Key Version Numbers in AuC Backup File

Procedure:

1. On the desktop, double-click the **Config Assistant** icon.
2. Perform one of the following actions:
 - To display information about key version numbers for the currently used database, enter: `ca keysreport`
 - To display information about key version numbers from the backup file, enter:
`ca keysreport -i <backup file name>`
Keys version report is displayed in the **CA** window.
3. Make notes of all Key Version numbers or print the file if possible. If these numbers do not match the numbers recorded in [AuC – Recording the Key Version Numbers on page 159](#), contact the ESSC for advice on how to manually synchronize keys.

9.2.4

AuC – Managing AuC Roles

Configuration Assistant tool is used to check and change AuC server current role.

It is possible to check AuC current role, change role from Active to Standby and the other way around.

9.2.4.1

Switching the Roles of the AuC Servers

If the server role is UNKNOWN, Config Assistant tries to set the role requested by the user.

Config Assistant does not proceed with changing role if network setup is incorrect (unknown IP address – not following the IP plan).

Procedure:

1. Log on to the Active AuC.
2. Double-click the **Config Assistant** icon on the desktop.
Config Assistant window opens.
3. Type `ca role standby`
4. Press `y`.

The following message appears:

Changing application role to STANDBY...

then the Active AuC will be shut down.

5. Use iGAS shut down command to permanently shut down AuC.

After the virtual machine is shut down, iGAS automatically tries to restart the application, which can lead to IP conflict. For detailed instructions on how to shut down application servers, see the *Network Management Servers* manual.

6. Log on to the Standby AuC.
7. Double-click the **Config Assistant** icon on the desktop.

Config Assistant window opens.

8. Type ca role active.

You are asked to confirm the operation.

9. Press y.

The following message appears:

Changing application role to ACTIVE...

It can take some time till the action is finished, then the server will be rebooted.

10. Log on to the Core Server's iGAS administration menu and boot the standby AuC. See the *Network Management Servers* manual.

9.2.4.1.1

Shutting Down Application Servers

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as instadm, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The following menu appears:

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

3. Enter the number associated with **Shutdown Application Servers**.

A list of application servers appears.

4. Enter the number associated with the particular application server you want to shut down.

9.2.4.2

Managing AuC Roles After Failure of Active AuC



IMPORTANT: To avoid possible IP conflicts, make sure that active AuC is shut down before proceeding with the activation procedure.

In case of failure of the AuC server, you need to change the role of the Standby AuC server to became Active. In such a case:

- Verify **Data currency** using Standby Manager GUI Client:
 - ◆ **IMPORTANT:** If both values displayed in **Last synchronized** and **Last changes applied** fields are **None** do not proceed with changing roles but reinstall Active_AuC and restore from backup file.
 - ◆ **NOTE:** Before proceeding with activation procedure consider data currency of the standby AuC (more recent date from **Last synchronized** and **Last changes applied** fields on Standby GUI Client). If you have newer backup file – reinstall active AuC and restore from that backup file.
- Change the role of the AuC B server (from Standby to Active) as per [Changing the Role of the Standby AuC to Active AuC on page 162](#).
- Perform required repairs to the damaged AuC A server
- On AuC A install AuC as Standby (choose the Standby option while installing AuC software)

To restore the original state (AuC A = Active, AuC B = Standby), perform [Switching the Roles of the AuC Servers on page 160](#).

9.2.4.3

Managing AuC Roles After Failure of Standby AuC

In case of failure of the Standby AuC server, reinstall the server from iGAS menu selecting standby option while reinstalling. You need to boot standby AuC from iGAS menu after the installation is finished. Database Standby manager is operating.

9.2.4.4

Changing the Role of the Standby AuC to Active AuC

Procedure:

1. Log on to the Standby AuC using the following IP address: 10.0.<ClusterOctet>.220
2. Double-click the **Config Assistant** icon on the desktop.
Config Assistant window opens.
3. Type **ca role active**.
You are asked to confirm the operation.
4. Press **y**.

The following message appears:

Changing application role to ACTIVE...

It can take some time till the action is finished, then the server will be rebooted.

Related Links

[Authentication Centre \(AuC\) Software Application Restoration on page 157](#)

9.3

AuC – Restoring Application

Prerequisites: Log on to the server as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)

- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to re-install Authentication Centre and enter: `n` for other applications.

The following message appears:

```
Please select AUC role: 1. Active 2. Standby
```

4. Enter the number reflecting the AuC role in the system.

The following message appears:

```
Shall Enhanced AuC be configured with PrC functionality disabled (y,n) [n]:
```

5. Enter: `y` or `n` accordingly.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

6. Log off from the server by entering `q`

7. Log on to the server using `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

8. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

9. Enter the number associated with **Boot Application Servers**.

10. Enter the number associated with Authentication Centre.

You have booted the application.

11. Enter: `q` and repeat this sequence until you log off from the server.

9.3.1

Installing the External Modem Driver for KVL to AuC/PrC Communication

Perform this procedure if you use the AuC/PrC to KVL modem connection. Otherwise, skip to the next procedure.

If you use the StarTech USB56KEMH2 modem, Windows automatically configures the connection. See “Configuring KVL Port Settings” in the *Authentication Centre (AuC) User Manual*. The modem should be attached and detached in out of service or disabled server mode.

Procedure:

1. Insert the *Enhanced Authentication Centre* DVD into the CD/DVD drive of the server hosting the AuC/PrC application.
2. Log on to iGAS as `instadm` by using one of the following procedures:
 - [Logging On to iGAS Through a Terminal Server on page 45](#)
 - [Logging On to iGAS Through a KVM Switch on page 48](#)
3. In the **Installation Administrator Main Menu**, enter the number for **Application Device Management**.
4. In the **Application Device Management**, enter the number for **Attach DVD to Application**.
5. In the **Attach DVD to Application**, enter the number for **Authentication Centre (auc_<X>.ucs<Y>)**, where <X> is the letter of the active AuC server and <Y> is the cluster number.
6. Stop the AuC/PrC services:
 - a. On the desktop, double-click the **Config Assistant** icon.
 - b. In the **Config Assistant** window, enter: `ca disable`
7. Right-click **Start** and select **Control Panel**.
8. In the **All Control Panel Items** window, select **Phone and Modem**.
9. If the **Location Information** window appears, enter the required information and click **OK**.
10. In the **Phone and Modem** window, select the **Modems** tab.
11. Click **Add**.
12. In the **Add Hardware Wizard** window, select the **Don't detect my modem; I will select it from a list** check box. Click **Next**.
13. Select **Have Disk**.
14. In the **Install From Disk** dialog box, select **Browse**.
15. On the *Enhanced Authentication Centre* DVD, navigate to `drivers\modem\MultitechA.INF`, and click **Open**.
16. In the **Install From Disk** dialog box, click **OK**.
17. From the **Models** list, select the **MultiTech MT9234ZBA** modem. Click **Next**.
18. Ensure that the **Selected ports** radio button is selected, and perform one of the following actions:
 - For AuC, select **COM1** and click **Next**.
 - For PrC, select **COM2** and click **Next**.The installation process starts, followed by the confirmation message.
19. Click **Finish**.

20. Log on to iGAS as `instadm`
21. In the **Installation Administrator Main Menu**, enter the number for **Application Device Management**.
22. In the **Application Device Management**, enter the number for **Detach DVD from Application**.
23. In the **Detach DVD from Application**, enter the number for **Authentication Centre (auc_<X>.ucs<Y>)**.
where <X> is the letter of the active AuC server and <Y> is the cluster number.
24. Start the AuC/PrC services:
 - a. On the desktop, double-click the **Config Assistant** icon.
 - b. In the **Config Assistant** window, enter: `ca enable`

Postrequisites: Ensure that the KVL ports are correctly configured. See “Configuring KVL Port Settings” in the *Authentication Centre (AuC) User Manual*.

Related Links

[Authentication Centre \(AuC\) Software Application Restoration](#) on page 157

9.4

AuC – Restoring Data from Backup

9.4.1

AuC – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: `https://master-uis.ucs/ui`
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [AuC – Uploading a Backup File to UIS on page 165](#). If the backup file already is in the UIS backup storage, continue to [Accessing Virtual Machines with the Web-Based Client on page 140](#).

9.4.2

AuC – Uploading a Backup File to UIS

Prerequisites: Log on to the Upgrade Console with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the Upgrade Console.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.



NOTE: If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Upload Files**.

The **Upload Files** screen appears.

2. Click **Browse**.

3. In the window that appears, select your backup file. Click **OK**.

 **NOTE:** The backup file is named `cluster<XX>_aucdb_01_<timestamp>`, where `<XX>` is the cluster ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

5. Click **Analyze Uploaded File**.

If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

9.4.3

Accessing Virtual Machines with the Web-Based Client

Procedure:

1. Open a web browser (Chromium).

2. In the address field, enter the IP address of the HostOS you want to access.

3. Perform the following actions:

- a. In the **User name** field, enter: `sysadmin`
- b. In the **Password** field, enter the password.
- c. Click **Log in**.

4. In the Web-based client, perform the following actions:

- a. In the **Navigator** pane, click **Virtual Machines**.

 **NOTE:** If a red exclamation mark is visible next to **System Time information** under the **System** tab in the **Navigator**, you can ignore it. To verify system time synchronization status, you can log in to IGAS as `sysadmin` user and use the **NTP Administration** menu.

- b. On the **Virtual Machines** list, select the check box next to the Virtual Machine you want to access.
- c. Select the **Consoles** tab.
- d. In the **Console Type** section, select **VNC**.

 **IMPORTANT:** Do not use other console types.

The graphical console appears in a new window.

 **NOTE:** If a VNC connection to virtual machine in Cockpit fails to pass keystrokes, you can press **CTRL+ALT+DEL**, and fold and unfold the virtual machine bar.

 **NOTE:** After a fresh installation or upgrade of CCE on DCS server, an unexpected Microsoft Windows dialog box appears, prompting you to restart your computer to apply the changes. You can ignore it or click **Restart Later**.

9.4.4

AuC – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: y
A message appears showing that the application server is disabled.
5. Enter q twice to go back to the **Application Servers Status Administration** menu.

9.4.5

AuC – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.
A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named `cluster<XX>_aucdb_01_<timestamp>`, where `<XX>` is the cluster ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyyymmddhhmm>`.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

9.4.6

AuC – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: `q` twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Authentication Centre \(AuC\) Software Application Restoration](#) on page 157

9.5

Replacing CryptR2

Procedure:

1. From NM Client, connect to the AuC server using the Remote Desktop.

2. Start the **Enhanced Authentication Centre Client**.

3. From the **System** menu, select **Go Out Of Service**.

The **Enhanced Authentication Centre Client** reports the **Out of Service** state of the server.

4. Disconnect the damaged CryptR2.

5. Configure the new CryptR2 device (IP and passwords) and connect it. For more information on setting up CryptR2, see the *Authentication Centre (AuC) User Manual*.

6. Load the CryptR2 Master Keys using KVL. See [Loading Keys with KVL](#) on page 170.

9.5.1

Displaying Current KVL Assignment

Perform this procedure to check the current serial port assignment for Key Variable Loader (KVL) communication.

Prerequisites: Log on as `instadm` using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **Application Device Management**.

The **Application Device Management** appears:

```
Application Device Management
-----
1. Display current device assignment
2. Attach device to Application
Please enter selection (1-2, q) [q]:
```

3. Enter the number for **Display current device assignment**.

The current port assignment appears.

9.5.2

Attaching KVL to Application

Perform this procedure to configure serial port 2 assignment for Key Variable Loader (KVL) communication if you are restoring a Core Server in the Primary Zone.

Prerequisites: Log on as `instadm` using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **Application Device Management**.

The **Application Device Management** menu appears:

```
Application Device Management
-----
1. Display current device assignment
2. Attach device to Application
Please enter selection (1-2, q) [q]:
```

3. Enter the number for **Attach device to Application**.
The **Attach device to Application** menu appears.
4. Enter the number for the application to which you want to attach serial port 2 for KVL communication.
The port assignment is changed and the **Application Device Management** menu appears.
5. To verify the current iGAS devices configuration, enter the number for **Display current device assignment**.

9.5.3

Loading Keys with KVL

Procedure:

1. In the Provisioning Centre Client, from the **System** drop-down menu, select **Encryption Devices**.
The client displays the encryption device with a status of **Not Loaded**.
2. In the **Encryption Device** window, click **Enter Password** and enter passwords for admin and user accounts.
3. Validate the passwords by clicking **Validate**.
4. Click **Enter AES Master Key** and enter the key. Click **OK**.
5. Click **Load Master Key** and select the DVI-XL key and KVL interface.
 - a. After clicking through the informational messages, the Provisioning Centre Client allows one minute to use the KVL to load the master key.
 - b. Using the key loading cable connect the KVL to the CryptR2.
 - c. From the main menu, select **Crypto Device** on the KVL.
 - d. From the list of available Master Keys, select a DVI-XL key to be loaded into the Crypto Device.

 **WARNING:** This must be the same DVI-XL Master Key as previously loaded, including the same DVI-XL system key associated to the Master Key. If you want to change the Master Key, see the *Provisioning Centre (PrC) User Manual*. ESSC should be notified.

A message appears confirming that the operation was successful.

6. In the **Encryption Device** window, click **Load Master Key** and select AES key and KVL interface.
 - a. After clicking through the informational messages, the Provisioning Centre Client allows one minute to use the KVL to load the master key.
 - b. From the main menu, select **Crypto Device** on the KVL.
 - c. From the list of available Master Keys, select AES 128 key to be loaded into the Crypto Device.A message appears confirming that the operation was successful.
7. Return to the PrC Client.
8. From the main PrC Client's menu, select **System** → **Go Operational**.

9.5.4

Loading Keys with Serial Connection

Procedure:

1. Open the **Enhanced Authentication Centre Client**. From the **System** drop-down menu, select **Encryption Devices**.
2. The **Enhanced Authentication Centre Client** displays the encryption device with a status of **Not Loaded**.
3. In the **Encryption Device** window, click **Enter Password** button, then enter passwords for admin and user accounts.
4. Click **Validate** button, to validate the passwords.
5. Click **Enter AES Master Key** button, then enter and confirm the key and click **OK**.
6. Click **Load Master Key** button, then select DVI-XL key and serial interface.
 - a. Once the informational messages have been clicked through, the **Enhanced Authentication Centre Client** allows one (1) minute to use the serial connection to load the master key.
 - b. Using the USB to Mini USB cable connect the service laptop to the CryptR2.
 - c. Establish a serial connection between the service laptop and CryptR2 using Com<X> port, where <X> is the serial port assigned to CryptR2. Use the following settings:
 - Baud rate: **9600**
 - Parity: **none**
 - Data bits: **8**
 - Stop bits: **1**
 - d. Log on as user
The `mkload>` prompt appears. You are prompted to enter the first master key.
 - e. Enter the first master key consisting of 128 hexadecimal digits.
You are prompted to enter the second master key.
 - f. Enter the second master key consisting of 16 hexadecimal digits.
A message confirming that the operation was successful appears.
 - g. Press **ENTER**.
 - h. Return to the **Enhanced Authentication Centre Client**.
Once the master key is loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.
7. In the **Encryption Device** window, click **Load Master Key** button, then select AES key and serial interface.
 - a. Once the informational messages have been clicked through, the **Enhanced Authentication Centre Client** allows one (1) minute to use the serial connection to load the master key.
 - b. Log on as user
The `mkload>` prompt appears. You are prompted to enter the master key.

- c. Enter the master key consisting of 32 hexadecimal digits.

A message confirming that the operation was successful appears.

- d. Return to the **Enhanced Authentication Centre Client**.

Once the master key is loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.

- e. Click **OK**.

 **WARNING:** This must be the same Master Key as stored in the **Enhanced Authentication Centre Client** Database. To change the Master Key, see the **Authentication Centre (AuC) User Manual** manual. ESSC should be notified.

8. Return to the **Enhanced Authentication Centre Client** and perform the following actions:

- a. From the main menu, select **System**.
- b. Select **Go Operational**.

Related Links

[Authentication Centre \(AuC\) Software Application Restoration](#) on page 157

9.6

AuC – Configuring Application

9.6.1

AuC – Restoring Keys After a Database Restore

This section describes restoring keys after a database restore. The following scenarios are covered:

- [AuC – Restoring Keys on a Single Cluster AuC](#) on page 172 – follow this procedure if you are restoring a single cluster AuC.
- [AuC – Restoring Keys on a Master AuC](#) on page 173 – follow this procedure if you are restoring a master AuC.
- [AuC – Restoring Keys on a Slave AuC](#) on page 174 – follow this procedure if you are restoring a slave AuC.

9.6.1.1

AuC – Restoring Keys on a Single Cluster AuC

Procedure:

1. Open the Authentication Centre client.
The configuration wizard appears.
2. In the **Confirm nationwide settings** window, select the **data is correct** radio button and click **Next**.
3. In the **Choose restoration type** window, select the **AuC will update (if necessary) keys in the system** radio button and click **Next**.

4. In the **Apply settings** window, set the *<Comm Key>* and *<Threshold>* values and confirm your settings by clicking the **Apply settings** button.



NOTE:

The Comm Key setting is not needed for the single cluster configuration.

The Threshold (Sites) value is set to 100% by default.

5. Click **Finish**.



NOTE:

Zone Controllers and BTSs connect to the Authentication Centre and report the version of keys they possess. It is illustrated in the **Max reported by device** field.

When the threshold is reached, you can check the versions of keys proposed by AuC.

The AuC client window appears with the **Restoring** tab opened.

A **Restore in progress - threshold not met** information is displayed in the **Restore Statistics** group.

6. Wait until the **Restore in progress - threshold met** confirmation appears in the **Restore Statistics** group.

The restoration process is completed.



NOTE: If any problems with CMG configuration are reported on this tab, contact ESSC for further assistance.

7. From the right-hand side of the **Restore Statistics** group, click the **Align keys** button.

8. In the **Confirmation** dialog box, click **OK**.

AuC begins the alignment of keys in the system.

9. Perform one of the following actions:

- If the **OTAR keys clearance confirmation** dialog box appeared, proceed to [AuC – Restoring Keys Troubleshooting on page 175](#).
- If the **OTAR keys clearance confirmation** dialog box did not appear, proceed to [AuC – Post-Restoration Checks on page 178](#).

9.6.1.2

AuC – Restoring Keys on a Master AuC

Procedure:

1. Open the Authentication Centre client on the restored Master AuC.

The nationwide settings configuration wizard appears.

2. In the **Confirm nationwide settings** window, select the **data is correct** radio button and click **Next**.

3. In the **Choose restoration type** window, select the **AuC will update (if necessary) keys in the system** radio button and click **Next**.

4. In the **Apply settings** window, set the **Comm Key** and **Threshold** values and confirm your settings by clicking the **Apply settings** button.

**NOTE:**

If backup contains outdated Comm Key material, set up a new Comm Key.

The Threshold (Sites) value is set to 100% by default.

A status message about connection of slave AuCs appears.

5. Wait until the message disappears and click **Finish**.

**NOTE:**

The AuC waits for all slave AuCs to connect for maximum 5 minutes.

- If no un-restored slave AuCs connected during this time, a failure message is displayed and the AuC will hang until at least one of the un-restored slave AuCs connect.
- If one or more un-restored slave AuCs connected during this time, the AuC client window with the **Restoring** tab appears. A **Restore in progress - threshold not met** information is displayed in the **Restore Statistics** group.

6. Wait for a **Restore in progress - threshold met** confirmation in the **Restore Statistics** group.

7. Click the **Accept Nationwide keys** button.

**IMPORTANT:**

Check all key versions which are proposed in **New Target** column and compare them to the key versions in **Max reported by devices** column.

If differences are found in CMG keys (GCK, TM-SCK, DM-SCK, GSKO) it is recommended to contact ESSC to evaluate possible consequences of accepting these keys. It might be the case that changing security class will be needed for such situation in a whole system.

8. In the **Confirmation** dialog box, click **OK**.

The keys restoration process is completed. The AuC client launches.

9. Perform one of the following actions:

- If the **OTAR keys clearance confirmation** dialog box appeared, proceed to [AuC – Restoring Keys Troubleshooting on page 175](#).
- If the **OTAR keys clearance confirmation** dialog box did not appear, proceed to [AuC – Post-Restoration Checks on page 178](#).

9.6.1.3

AuC – Restoring Keys on a Slave AuC

Procedure:

1. Open the Authentication Centre client on the restored machine.
The nationwide settings configuration wizard appears.
2. In the **Confirm nationwide settings** window, select the **data is correct** radio button and click **Next**.
3. In the **Choose restoration type** window, select the **AuC will update (if necessary) keys in the system** radio button and click **Next**.

4. In the **Apply settings** window, set the **Comm Key** and **Threshold** values and confirm your settings by clicking the **Apply settings** button.



NOTE:

If backup contains outdated Comm Key material, set up a new Comm Key.

The Threshold (Sites) value is set to 100% by default.

A status message about the connection to the Master AuC appears.

5. After the connection with master AuC is established click the **Finish** button.

The AuC client window with the **Restoring** tab opened appears.

A **Restore in progress - threshold not met** information is displayed in the **Restore Statistics** group.

6. Wait for a **Restore in progress - threshold met** confirmation in the **Restore Statistics** group.

7. Click the **Accept Nationwide keys** button.



IMPORTANT:

Check all key versions which are proposed in **New Target** column and compare them to the key versions in **Max reported by devices** column.

If differences are found in CMG keys (GCK, TM-SCK, DM-SCK, GSKO) it is recommended to contact ESSC to evaluate possible consequences of accepting these keys. It might be the case that changing security class will be needed for such situation in a whole system.

8. In the **Confirmation** dialog box, click **OK**.

The keys restoration process is completed. The AuC client launches.

9. Perform one of the following actions:

- If the **OTAR keys clearance confirmation** dialog box appeared, proceed to [AuC – Restoring Keys Troubleshooting on page 175](#).
- If the **OTAR keys clearance confirmation** dialog box did not appear, proceed to [AuC – Post-Restoration Checks on page 178](#).

9.6.1.4

AuC – Restoring Keys Troubleshooting

During the process of key alignment, the following scenarios may appear:

- GSKO has advanced in crypto period and at least one depending key has also advanced in crypto period, compared to the keys in the backup.
- GSKO is identical to the GSKO in the backup, but GCK and possible TM-SCK or DM-SCK keys have advanced in crypto period.

If the system is in SC3G then sites fallback to SC3 until the key restoration process is completed.

Procedure:

1. In the **OTAR keys clearance confirmation** dialog box, click **OK**.

The **OTAR keys handling** group appears in the upper right-hand corner of the **Restoring** tab.

Figure 11: OTAR Keys Handling Group Box

 **NOTE:** You can monitor the tasks AuC is performing during the process of key alignment in the **Restore Statistics** group.

2. In the **OTAR keys handling** group, from the drop-down menu, select the preferred activation method.

 **NOTE:** For illustrative purposes, the **Manual** type of activation is detailed in the next steps of this procedure. This type of activation demands the user to trigger the OTAR activation manually.

Once the OTAR activation type is selected, the **Clear OTAR** button (located next to the drop-down menu) becomes active.

3. Click the **Clear OTAR** button.
4. In the **Restore stage confirmation** dialog box, click the **Yes** button.

Authentication Centre determines whether only the GCK keys, or the GCK, TM-SCK, and DM-SCK keys need clearing in the Base Sites. The application demands actions from the user accordingly.

5. Optional: If AuC clears only the GCK keys, then wait for the GCK threshold for Base Sites to be reached and proceed to [step 8](#).

 **NOTE:**

You can expedite the restoration by pressing the **Send OTAR / Send GSKO** button, but this does not speed up the key synchronization process.

You can repeat this action for all types of keys.

AuC clears the OTAR GCK keys in Base Sites.

6. Wait for the threshold for Base Sites to be reached.

AuC is clearing OTAR GCK, TM-SCK, DM-SCK keys in Base Sites.

7. Wait for the OTAR GSKO threshold for Mobile Stations to be reached.

AuC sends OTAR GSKO keys to Zone Controllers.

8. Wait for the OTAR GCK threshold for Mobile Stations to be reached.

 **NOTE:** During the Manual restoration, click the **Activate OTAR** button to finish the process (irrespective of whether the threshold was reached, or not).

OTAR is activated, the key restoration process is completed and support for SC3G is restored.

The **AuC Restoring** tab disappears.

9.6.2

AuC – Ensuring That the AuC Is Operational After Restoration

Procedure:

1. Double click the **Config Assistant** icon on the desktop.
2. Enter: `ca status -v` and verify if AuC services are running. If not, enter: `ca enable` to start them.
3. Log on to the AuC Client.
4. Make sure the CryptR2 has been detected and is usable. From the main menu select **SystemEncryption Device**. The CCC and CCE version must be correct, and the device status must be **Working**. If these requirements are not fulfilled, the problem MUST be resolved before proceeding.
 **NOTE:** The possible causes of CryptR2 failure are as follows:
 - no Master Key has been loaded into the CryptR2
 - Windows driver for the CryptR2 has not been installed
5. Ensure the AuC operational state is set to **Operational**.
 **NOTE:** If the AuC operational service is **Out of Service**, from the main menu select **System Go Operational**.

9.6.3

AuC – Cleaning Up the AuC Database

Procedure:

1. Double click the **Config Assistant** icon on the desktop.
2. Enter: `ca disable`
3. Enter: `ca enable -d`
4. Enter: `ca dbreset`
You are prompted to confirm the command.
5. Enter: `y`
Wait while the database is cleaned up. Command prompt appears.
6. Close **Config Assistant** window.

Result:

 **NOTE:** After performing this procedure, AuC looks like only just installed application and requires configuration.

Related Links

[Authentication Centre \(AuC\) Software Application Restoration on page 157](#)

9.7

AuC – Installing and Configuring RSA Authentication Software

Procedure:

1. Clear 2FA Secret key on the RSA server. See the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.



IMPORTANT:

When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

The RSA Agent installation should be performed after the promoting of Domain Controller.

Related Links

[Authentication Centre \(AuC\) Software Application Restoration](#) on page 157

9.8

AuC – Post-Restoration Checks

Table 33: AuC – Post-Restoration Checks

Action	Post-Restoration Checks
AuC restoration - all procedures	<p>Check if the UCS and ZDSs are connected. Use the Synchronization tab on the AuC Client.</p> <p>Check statuses of ZCs and base sites. Use the Devices tab on the AuC Client.</p> <p>Check in the Schedules tab that active and inactive keys are as expected.</p> <p>At a time agreed with users, ensure at least two key updates are successful.</p> <p>Check also that AuC came back green and OK in UEM.</p>

Related Links

[Authentication Centre \(AuC\) Software Application Restoration](#) on page 157

9.9

AuC – Backup Procedures

A user that has database management permissions can start a backup on demand from the AuC client.

Be aware of available disk space and remove old backups when no longer needed. Single backup can take ~0.5GB – so if old backups are not deleted they can use all available disk space.



NOTE:

Scheduled backup, if started in the middle of important action (like key updates, CMG edits, etc) will not be very useful. Manual backups should be executed when the AuC database is stable state.

You must log on the NM Client as **motosec** user in order to be able to connect to the AuC Server.

Before starting backup ensure that AucPgSvcR09xxxxx service is running using the `ca status -v` command from the **Config Assistant** tool.

9.9.1

AuC – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

9.9.1.1

AuC – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

9.9.1.2

AuC – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **auc_active** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the AuC application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **auc_active** application in the **Use Central Storage** column. Make sure that you select the check box for the AuC in the correct zone.

 **NOTE:** For redundant applications, the active application is indicated by the postfix **_active** in the name.

4. If you want to save the backup file in the Storage PC, select the check box of the **auc_active** application in the **Use Storage PC** column.

 **NOTE:** The backup file is cumulatively added to the backups on the Storage PC.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [AuC – Backing Up Data On-Demand on page 180](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [AuC – Scheduling Backup on page 181](#).
- You can do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

9.9.1.3

AuC – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **auc_active** application in the relevant zone, click **Run**.

 **NOTE:** For redundant applications, the active application is indicated by the postfix **_active** in the name.

 **NOTE:**

You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

When the backup task is initiated, the Enhanced Software Update tool finds out whether any of the redundant applications are active. If there is an active application, the backup is performed for this application. If none of the redundant applications are active, the backup fails.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [AuC – Scheduling Backup on page 181](#).
- If you want to save the backup file on the NM Client PC, continue to [AuC – Downloading a Backup File to the NM Client PC on page 182](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

9.9.1.4

AuC – Scheduling Backup

Prerequisites: Log on the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

a. In the **Name** field, type a name for the scheduled backup task.

b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **auc_active** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

c. In the **Day** drop-down list, select a week day or select **DAILY**.

d. In the **Hour** drop-down list, select at which hour the backup must run.

- e. In the **Minute** drop-down list, select at which minute the backup must run.
- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [AuC – Downloading a Backup File to the NM Client PC on page 182](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

9.9.1.5

AuC – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `cluster<XX>_aucdb_01_<timestamp>.tar.gz`, where `<XX>` is the cluster ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Chapter 10

System Statistics Server (SSS) – Software Application Restoration

Table 34: SSS – Restoration References

Action	Reference	Done
Software restoration	SSS – Restoration Impact on page 183	
	SSS – Pre-Restoration Checks on page 183	
	SSS – Restoring Application on page 184	
	SSS – Configuring Application on page 185	
	SSS – Restoring Data from Backup on page 186	
	SSS – Installing and Configuring RSA Authentication Software on page 189	
	SSS – Post-Restoration Checks on page 189	
	SSS – Backing Up Data on page 189	

10.1

SSS – Restoration Impact

Table 35: SSS – Restoration Impact

Action	Service Affected	Service Downtime
Software restoration	SSS unavailable - no system historical reports kept for duration of restoration.	Approximately 2 hours.

10.2

SSS – Pre-Restoration Checks

Table 36: SSS – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	Take a new backup if the previous one is not available for use.
	Check if the reported problem still exists.
	Check the Time Zone.

Action	Pre-Restoration Checks
	Make sure that the application server is disabled prior to software restoration. Perform SSS – Disabling the Application Server on page 184 .

10.2.1

SSS – Disabling the Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with **Application Servers Status Administration**.
4. Enter the number associated with **Disable Application Servers**.
5. Enter the number associated with the application server that you want to disable.
6. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

Related Links

[System Statistics Server \(SSS\) – Software Application Restoration on page 183](#)

10.3

SSS – Restoring Software

10.3.1

SSS – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to re-install **System Statistics Server**, and enter: `n` for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering `q`
5. Log on to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number for **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number for **System Statistics Server**.

You have booted the System Statistics Server application.

9. Enter: `q` and repeat this sequence until you log off from the server.

10. Continue to the next section.

Related Links

[System Statistics Server \(SSS\) – Software Application Restoration](#) on page 183

10.3.2

SSS – Configuring Application

The following describes how to properly configure the System Statistics Server (SSS) application server.

10.3.2.1

SSS – Enabling the Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: `q` twice to go back to the **Application Servers Status Administration** menu.

Related Links

[System Statistics Server \(SSS\) – Software Application Restoration on page 183](#)

10.4

SSS – Restoring Data from Backup

10.4.1

SSS – Logging On to the Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
```

```
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with the **SSS Server**.

The login prompt appears.

4. Log in as `ssssadmin`.

The server application's menu appears.

10.4.2

SSS – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: `y`
A message appears showing that the application server is disabled.
5. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

10.4.3

SSS – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named zone<XX>_sssdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

10.4.4

SSS – Enabling the Application Server

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: **q** twice to go back to the **Application Servers Status Administration** menu.

Related Links

[System Statistics Server \(SSS\) – Software Application Restoration on page 183](#)

10.5

SSS – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.



IMPORTANT: When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[System Statistics Server \(SSS\) – Software Application Restoration](#) on page 183

10.6

SSS – Post-Restoration Checks

Table 37: SSS – Post-restoration Checks

Action	Post-Restoration Checks
Software restoration	<ul style="list-style-type: none">● Historical Reports● ATR● RCM including CADI/Multi-CADI● System Health Application Suite● Unified Event Manager● ATIA

10.7

SSS – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

10.7.1

SSS – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

10.7.2

SSS – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console. A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **sss01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the SSS application in the correct zone.
 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.
3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **sss01** application in the **Use Central Storage** column. Make sure that you select the check box for the SSS in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **sss01** application in the **Use Storage PC** column.
 **NOTE:** The backup file is cumulatively added to the backups on the Storage PC.
5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [SSS – Backing Up Data On-Demand on page 191](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [SSS – Scheduling Backup on page 191](#).
- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

10.7.3

SSS – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **sss01** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The Backup Status column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [SSS – Scheduling Backup on page 191](#).
- If you want to save the backup file on the NM Client PC, continue to [SSS – Downloading a Backup File to the NM Client PC on page 192](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

10.7.4

SSS – Scheduling Backup

Prerequisites: Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Perform the following actions:
 - a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **sss01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.
- d. In the **Hour** drop-down list, select at which hour the backup must run.
- e. In the **Minute** drop-down list, select at which minute the backup must run.
- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [SSS – Downloading a Backup File to the NM Client PC on page 192](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

10.7.5

SSS – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named zone<XX>_sssdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[System Statistics Server \(SSS\) – Software Application Restoration](#) on page 183

Chapter 11

User Configuration Server (UCS) – Software Application Restoration

This table contains references to procedures to be performed to restore and back up the User Configuration Server (UCS) application server. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 38: User Configuration Server – Restoration References

Action	Reference	Done
Software restoration	UCS – Restoration Impact on page 194	
	UCS – Pre-Restoration Checks on page 195	
	UCS – Restoring Application on page 196	
	UCS – Configuring Application on page 197	
	UCS – Restoring Data from Backup on page 198	
	UCS – Installing and Configuring RSA Authentication Software on page 203	
	UCS – Post-Restoration Checks on page 203	
	UCS – Backing Up Data on page 206	

11.1

UCS – Restoration Impact

Table 39: UCS – Restoration Impact

Action	Service Affected	Service Downtime
Database Restoration through Enhanced Software Update tool	<ul style="list-style-type: none"> UCS unavailable All ZDSes disabled to synchronize the databases with UCS. <p>Nationwide RCM data changes cannot be populated to this clusters ATR servers.</p>	Up to 1h for UCS restore, then up to 1h for the synch down procedure.
Database Restoration directly from a backup file	<ul style="list-style-type: none"> UCS unavailable All ZDSes disabled to synchronize the databases with UCS. <p>Nationwide RCM data changes cannot be populated to this clusters ATR servers.</p>	Up to 1h for UCS restore, then up to 1h for the synch down procedure.

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.2

UCS – Pre-Restoration Checks

Table 40: UCS – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	<p>Check system IP Plan</p> <p>Multi-CADI</p> <p> NOTE: Multi-CADI still functions if UCS and ZDS are down, only new logons are not possible when the ZDS is down (required for restoring the UCS database).</p>
	<p>Check for READY/READY status of replication.</p>
	<p>Check trunking status and Security Class Status of BTS sites are at correct level before the UCS restoration (if the security class restoration level is critical).</p>
	<p>Ensure that AuC is Operational and In Service and remains in service for the duration of the UCS restoration. Also check AuC shows status of sites correctly and ZC has correct sites wide.</p>
	<p>Make sure that the ZDS, UCS, and ATR application servers are disabled prior to software restoration. Perform UCS – Disabling Application Server on page 195.</p>

11.2.1

UCS – Disabling Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server](#) on page 45
- [Logging On to iGAS Through a KVM Switch](#) on page 48

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with **Application Servers Status Administration**.
4. Enter the number associated with **Disable Application Servers**.
5. Enter the number associated with the application server that you want to disable.
6. Enter **q** twice to go back to the **Application Servers Status Administration** menu.

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.3

UCS – Restoring Software

11.3.1

UCS – Restoring Application

Prerequisites: Log on to the server as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: **y** when the installer prompts you to re-install **User Configuration Server**, and enter: **n** for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering **q**

5. Log on to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
```

```
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number associated with **User Configuration Server**.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter: q and repeat this sequence until you log off from the server.

10. Continue to the next section.

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.3.2

UCS – Configuring Application

11.3.2.1

UCS – Enabling the Application Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server](#) on page 45
- [Logging On to iGAS Through a KVM Switch](#) on page 48

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.

3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

11.4

UCS – Restoring Data from Backup

Perform the following procedures to restore the UCS database.

 **IMPORTANT:** If you are performing both UCS and ZDS restoration, ensure that UCS is restored before ZDS.

11.4.1

UCS – Logging On to the Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with the **UCS Server**.

The login prompt appears.

4. Log in as `ucadmin`.

The server application's menu appears.

11.4.2

UCS – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.

4. If prompted for confirmation, enter: y
A message appears showing that the application server is disabled.
5. Enter q twice to go back to the **Application Servers Status Administration** menu.

11.4.3

UCS – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named `cluster<XX>_ucsdb_01_<timestamp>.tar.gz`, where `<XX>` is the cluster ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

11.4.4

UCS – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

System Administrator Main Menu

```

1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:

```

2. Enter the number for **Application Servers Status Administration**.

3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

Postrequisites: Synchronize Zone Database with UCS. See [ZDS – Synchronizing Zone Database with UCS on page 204](#).

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.5

UCS – Exporting Radio Control Manager Data

Perform this procedure to export the RCM data. For multi-cluster systems, perform this procedure for all clusters.

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```

System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:

```

2. Enter the number associated with **Application Servers Administration Menus**.

The **Application Servers Administration Menus** appear.



NOTE: The list of available servers varies depending on the deployment type.

3. Enter the number associated with the **UCS application server**.

The login prompt appears.

4. Log on as ucadmin.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Confirm by pressing **ENTER** and answer the application server's initial prompts.

You are logged on, and the **User Configuration Server Administration** menu appears.

```
User Configuration Server Administration 1. Enable User Configuration Server 2.  
Enable User Configuration Server (fast) 3. Disable User Configuration Server 4.  
Display Server Status 5. Database Administration 6. Feature Administration 7.  
Unix Administration 8. Backup Server Administration 9. Multiclusler Radio Control  
Manager Administration 10. UCS Report Administration Enter Selection: (1-10, q, ?)  
[q]>
```

6. Enter the number associated with **Multiclusler Radio Control Manager Administration**.

The **Multiclusler Radio Control Manager Administration** menu appears:

```
Multiclusler Radio Control Manager Administration 1. Export Radio Control Manager  
Data 2. Collect and Combine Radio Control Manager Data 3. Configure Automatic  
Radio Control Manager Export 4. Configure Automatic Collect and Combine of Radio  
Control Manager Export 5. Enable Automatic Export, Collect and Combine of Radio  
Control Manager Data 6. Disable Automatic Export, Collect and Combine of Radio  
Control Manager Data 7. Display Status of Radio Control Manager Operations 8.  
Display History of Radio Control Manager Operations Enter Selection: (1-8,,q, ?):
```

7. Enter the number associated with **Export Radio Control Manager Data**.

The following exemplary message indicates that the action is complete:

```
2016-08-04 18:03:51| Export of Multiclusler RCM data completed successfully...
```

8. Return to the **Server Administration** menu by entering **q**

11.6

UCS – Collect and Combine

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu  
-----  
1. Enable all Application Servers  
2. Disable all Application Servers  
3. Display Status of all Application Servers  
4. Unix Administration  
5. Application Servers Administration Menus  
6. Application Servers Boot/Reboot/Shutdown  
7. Application Servers Status Administration  
8. Application Isolation Management  
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

The **Application Servers Administration Menus** appear.



NOTE: The list of available servers varies depending on the deployment type.

3. Enter the number associated with the UCS application server.

The login prompt appears.

4. Log in as ucadmin.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Confirm by pressing **ENTER** and answer the application server's initial prompts.

You are logged on, and the **User Configuration Server Administration** appears.

```
User Configuration Server Administration 1. Enable User Configuration Server 2.
Enable User Configuration Server (fast) 3. Disable User Configuration Server 4.
Display Server Status 5. Database Administration 6. Feature Administration 7.
Unix Administration 8. Backup Server Administration 9. Multicloud Radio Control
Manager Administration 10. UCS Report Administration Enter Selection: (1-10, q, ?)
[q]>
```



IMPORTANT: In multicloud systems that include servers which do not support security mode, you need to perform [step 6](#) through [step 9](#) to disable security mode on all servers. This ensures the collect and combine operation success. In other scenarios, you can go to [step 10](#).

6. Enter the number for **Unix Administration**.

The **Unix Administration** menu appears.

7. Enter the number for **Toggle security mode**.

8. At the prompt to confirm disabling the security mode, enter: **Y**

9. Return to the **User Configuration Server Administration** menu.

10. Enter the number associated with **Multicloud Radio Control Manager Administration**.

The **Multicloud Radio Control Manager Administration** menu appears:

```
Multicloud Radio Control Manager Administration 1. Export Radio Control Manager
Data 2. Collect and Combine Radio Control Manager Data 3. Configure Automatic
Radio Control Manager Export 4. Configure Automatic Collect and Combine of Radio
Control Manager Export 5. Enable Automatic Export, Collect and Combine of Radio
Control Manager Data 6. Disable Automatic Export, Collect and Combine of Radio
Control Manager Data 7. Display Status of Radio Control Manager Operations 8.
Display History of Radio Control Manager Operations Enter Selection: (1-8, ,q, ?):
```

11. Enter the number associated with **Collect and Combine Radio Control Manager Data**.

The following exemplary message indicates that the action is complete:

```
2016-07-26 19:12:07| Transfer and merge of Multicloud RCM data completed
successfully... 2016-07-26 19:12:08| Data distribution to the ATR servers is in
progress. You can check its status from the menu.
```

12. Return to the Server Administration menu by entering **q**

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.7

UCS – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.8

UCS – Post-Restoration Checks

Table 41: UCS – Post-Restoration Checks

Action	Post-Restoration Checks
Software restoration	Make sure the following procedures are performed: <ol style="list-style-type: none">1. UCS – Collect and Combine on page 1292. ZDS – Disabling the Application Server on page 2043. Enabling Application Servers on page 2064. ZDS – Checking SDR Database Synchronization on page 205
	Check if AuC has synchronized with UCS and Zone Manager.
	Check if UCM, and SWDL are both operational from PRNM suite.
	Check that System Historical Reports are being populated as expected.
	Check the Security Class status of the system after the database restore (check that Key Material has synchronized successfully from the AuC).
	Check that the Unified Event Manager reports the correct status for all connected entities.
	Check if MTIG-IP server is working correctly. If UCS restoration caused MTIG-IP NM configuration change, MTIG-IP reboot is required so that the change is applied. For more information on rebooting MTIG-IP server, see Rebooting the MTIG-IP Server on page 267.

11.8.1

ZDS – Disabling the Application Server

Prerequisites: Before you start this procedure, you must be logged in to the server, and the **System Administrator Main Menu** menu must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the Zone Database Server application server.
A message appears showing that the application server is disabled.
4. Enter q twice to go back to the **Application Servers Status Administration** menu.

11.8.2

ZDS – Synchronizing Zone Database with UCS

Use this procedure whenever synchronizing Zone Database with UCS is necessary, for example in case of corruption of the Zone Database.

Prerequisites: Disabling ZDS is required for this procedure. Disabling of the UCS and optimization of its database is recommended.

Log on to iGAS as sysadmin. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

The **Application Servers Administration Menus** appear.

3. Enter the number associated with the ZDS application server.

The login prompt appears.

4. Log on as dsadmin.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Enter the number associated with **Database Administration**.

6. Enter the number associated with **Synchronize Zone Database with UCS**.



IMPORTANT: The ZDS must be disabled at this point.

The ZDS database is synchronized with UCS and a string of messages is displayed.

7. Enter: q until logged out of the application server and back to iGAS.

Postrequisites:

- Ensure the output does not communicate any errors. If you see error messages, contact your Motorola Solutions representative.
- Enable ZDS and continue to the next procedure.

11.8.3

ZDS – Checking SDR Database Synchronization

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q] :
```

2. Type the number associated with **Application Servers Administration Menus** and press **Enter**.

The list of servers appears.



NOTE: The list of available servers varies depending on the deployment type.

3. Type the number associated with the SDR application server and press **Enter**.

The login prompt appears.

4. Log in as sdr_mgr.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Confirming by pressing **Enter**, answer the application servers initial prompts.

You are logged on, and the SDR Server Administration menu appears.

6. If redundant SDR, then ensure via the `srs_status` command that this is the Active SDR.

7. Type config to start the configuration interface.
8. Go to **Data Distribution Interface** and then **View/Modify DDI Server**.
9. Select the UCS server from menu and check the UCS synchronization has completed:

Exemplary output:

```
Started
Finished
Full sync : 02/09/08 16:16:00 02/09/08 16:16:03
Completed
```

10. Select the **ZDS** server from the menu and check the ZDS synchronization has completed as well.
11. In case UCS or ZDS synchronization has not completed, then use the appropriate **Synchronize to** menu entry in the Data Distribution Interface menu to start the synchronization.

11.8.4

Enabling Application Servers

You enable and disable application servers from their respective administration menus. Enabling a server starts all of the processes necessary for the server to function properly in the system.

Normally, you do not have to enable an application server because its normal state is enabled. A server may need to be enabled if it was disabled earlier. If you must enable a particular server, follow this procedure.

Procedure:

1. Enter the number associated with the server you want to enable.
You are prompted for the user password on the application server you want to enable.
2. Enter the password.
 **NOTE:** The initial administrative prompts vary depending on the application server in question.
The application server displays initial administrative prompts.
3. Confirming by pressing ENTER, answer the application servers initial prompts.
You are logged on, and the Administration menu for the server you have chosen appears.
4. Enter the number associated with **Enable Server Name Server**.
Process messages appear that indicate the server has been enabled, followed by the server's Administration menu.

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

11.9

UCS – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

11.9.1

UCS – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

11.9.2

UCS – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.
A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **ucs01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the UCS application in the correct zone.
 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.
3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **ucs01** application in the **Use Central Storage** column. Make sure that you select the check box for the UCS in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **ucs01** application in the **Use Storage PC** column.
 **NOTE:** The backup file is cumulatively added to the backups on the Storage PC.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [UCS – Backing Up Data On-Demand on page 208](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [UCS – Scheduling Backup on page 208](#).

- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

11.9.3

UCS – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **ucs01** application in the relevant zone, click **Run**.



NOTE: You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [UCS – Scheduling Backup on page 208](#).
- If you want to save the backup file on the NM Client PC, continue to [UCS – Downloading a Backup File to the NM Client PC on page 209](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

11.9.4

UCS – Scheduling Backup

Prerequisites: Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

a. In the **Name** field, type a name for the scheduled backup task.

b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **ucs01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

c. In the **Day** drop-down list, select a week day or select **DAILY**.

d. In the **Hour** drop-down list, select at which hour the backup must run.

e. In the **Minute** drop-down list, select at which minute the backup must run.

f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [UCS – Downloading a Backup File to the NM Client PC on page 209](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

11.9.5

UCS – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `cluster<XX>_ucsdb_01_<timestamp>.tar.gz`, where `<XX>` is the cluster ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[User Configuration Server \(UCS\) – Software Application Restoration](#) on page 194

Chapter 12

License Manager – Software Application Restoration

This table contains references to procedures to perform to restore and back up the License Manager application server. Perform the procedures in the order specified in the table.

 **NOTE:** The backup contains all customizations performed by the user since the installation of License Manager, including installed licenses.

12.1

License Manager – Restoration Impact

Table 42: License Manager – Restoration Impact

Action	Service Affected	Service Downtime
Database Restoration through Enhanced Software Update tool	<ul style="list-style-type: none">License Manager unavailable – no changes in license information are possible	Up to 1h for License Manager restore.
Database Restoration directly from a backup file	<ul style="list-style-type: none">License Manager unavailable – no changes in license information are possible	Up to 1h for License Manager restore.

12.2

License Manager – Pre-Restoration Checks

Table 43: License Manager – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	<p>Check system IP Plan</p> <p>Make sure that the License Manager application server is disabled prior to software restoration. Perform License Manager – Disabling Application Server on page 211.</p>

12.2.1

License Manager – Disabling Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. At the prompt, enter a short description of why you want to access the server. As stated on the screen, you must enter a full stop in the left-most position of a line to end the description.

The **System Administrator Main Menu** menu appears.

3. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

4. Enter the number associated with **Application Servers Status Administration**.
5. Enter the number associated with **Disable Application Servers**.
6. Enter the number associated with the application server that you want to disable.
7. Enter q twice to go back to the **Application Servers Status Administration** menu.

12.3

License Manager – Restoring Software

12.3.1

License Manager – Restoring Application

Prerequisites: Log on to the server as instadm. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as instadm, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: y when the installer prompts you to re-install **License Manager**, and enter: n for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering q
5. Log on to the server using the sysadmin login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number associated with **License Manager**.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter: q and repeat this sequence until you log off from the server.

10. Continue to the next section.

12.3.2

License Manager – Enabling the Application Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

12.4

License Manager – Restoring Data from Backup

Perform the following procedures to restore the License Manager database.

12.4.1

License Manager – Disabling Application Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. At the prompt, enter a short description of why you want to access the server. As stated on the screen, you must enter a full stop in the left-most position of a line to end the description.

The **System Administrator Main Menu** menu appears.

3. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

4. Enter the number associated with **Application Servers Status Administration**.

5. Enter the number associated with **Disable Application Servers**.

6. Enter the number associated with the application server that you want to disable.

7. Enter q twice to go back to the **Application Servers Status Administration** menu.

12.4.2

License Manager – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named `cluster<XX>_lmbd_01_<timestamp>.tar.tgz` or `zone<XX>_lmbd_01_<timestamp>.tar.tgz`, where `<XX>` is the cluster ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

12.4.3

License Manager – Enabling the Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: **q** twice to go back to the **Application Servers Status Administration** menu.

12.5

License Manager – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

12.5.1

License Manager – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

12.5.2

License Manager – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone License Manager, select the check box of the **lm01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the UCS application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the Storage PC, select the check box of the **lm01** application in the **Use Storage PC** column.

 **NOTE:** The backup file is cumulatively added to the backups on the Storage PC.

4. Click Apply changes.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [UCS – Backing Up Data On-Demand on page 208](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [UCS – Scheduling Backup on page 208](#).
- You can do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

12.5.3

License Manager – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **lm01** application in the relevant zone, click **Run**.



NOTE: You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [UCS – Scheduling Backup on page 208](#).
- If you want to save the backup file on the NM Client PC, continue to [UCS – Downloading a Backup File to the NM Client PC on page 209](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

12.5.4

License Manager – Scheduling Backup

Prerequisites: Log on the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

- a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **lm01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.

- d. In the **Hour** drop-down list, select at which hour the backup must run.

- e. In the **Minute** drop-down list, select at which minute the backup must run.

- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [UCS – Downloading a Backup File to the NM Client PC on page 209](#). Otherwise, you do not have to do anything else regarding backup.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

12.5.5

License Manager – Downloading a Backup File to the NM Client PC

Prerequisites:



IMPORTANT: If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.



NOTE: If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.



IMPORTANT: The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.



NOTE: The backup file is named cluster <XX>_lmdb_01_<timestamp>.tar.gz or zone <XX>_lmdb_01_<timestamp>.tar.gz, where <XX> is the cluster ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.



NOTE: You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.

4. In the **Save As** window, select a location for the file and click **Save**.

Chapter 13

Unified Event Manager (UEM) – Software Application Restoration

This table contains references to procedures to be performed to restore and back up the Unified Event Manager (UEM) application server. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 44: Unified Event Manager – Restoration References

Action	Reference	Done
Software restoration	UEM – Restoration Impact on page 220	
	UEM – Pre-Restoration Checks on page 220	
	UEM – Restoring Application on page 221	
	UEM – Configuring Application on page 223	
	UEM – Restoring Data from Backup on page 223	
	UEM – Installing and Configuring RSA Authentication Software on page 226	
	UEM – Post-Restoration Checks on page 226	
	UEM – Backing Up Data on page 226	

13.1

UEM – Restoration Impact

Table 45: UEM – Restoration Impact

Action	Service Affected	Service Downtime
Software restoration	Fault management services are unavailable. System Health Application Suite is not reporting states of sites.	Depends on restoration time and database size.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration on page 220](#)

13.2

UEM – Pre-Restoration Checks

Table 46: UEM – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	Take a new backup if the previous one is not available for use.

Action	Pre-Restoration Checks
	Check if the reported problem still exists.
	Check the Time Zone.
	Make sure that the application server is disabled prior to software restoration. Perform UEM – Disabling Application Server on page 221 .

13.2.1

UEM – Disabling Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q] :
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with **Application Servers Status Administration**.
4. Enter the number associated with **Disable Application Servers**.
5. Enter the number associated with the application server that you want to disable.
6. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration on page 220](#)

13.3

UEM – Restoring Software

13.3.1

UEM – Restoring Application

Prerequisites: Log on to the server as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)

- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to re-install **Unified Event Manager Server**, and enter: `n` for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering `q`

5. Log on to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number associated with **Unified Event Manager Server**.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter: `q` and repeat this sequence until you log off from the server.

10. Continue to the next section.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration on page 220](#)

13.3.2

UEM – Configuring Application

No additional configuration is required. If you are not restoring data from backup, perform [UEM – Enabling the Application Server on page 223](#).

13.3.2.1

UEM – Enabling the Application Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

Postrequisites: If attempts to launch the UEM client after switchover fail, follow the “Clear the Java Cache” procedure from the *Unified Event Manager* manual.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration on page 220](#)

13.4

UEM – Restoring Data from Backup

Perform the following procedures to restore the database from backup. Ensure that the application server is disabled before you begin the restoration process.

13.4.1

UEM – Logging On to the Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with the **UEM Server**.

The login prompt appears.

4. Log on as `uemadmin`.

The server application's menu appears.

13.4.2

UEM – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: `y`
A message appears showing that the application server is disabled.
5. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

13.4.3

UEM – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named zone<XX>_uemdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymddhhmm>.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

13.4.4

UEM – Enabling the Application Server

Prerequisites:

Log on to the server as sysadmin by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration](#) on page 220

13.5

UEM – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.



IMPORTANT: When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration](#) on page 220

13.6

UEM – Post-Restoration Checks

Table 47: UEM – Post-Restoration Checks

Action	Post-Restoration Checks
Software restoration	N/A

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration](#) on page 220

13.7

UEM – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

13.7.1

UEM – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

13.7.2

UEM – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.
A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **uem01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the UEM application in the correct zone.



NOTE: You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **uem01** application in the **Use Central Storage** column. Make sure that you select the check box for the UEM in the correct zone.
4. If you want to save the backup file in the Storage PC, select the checkbox of the **uem01** application in the **Use Storage PC** column.



NOTE: The backup file is cumulatively added to the backups on the Storage PC.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [UEM – Backing Up Data On-Demand on page 228](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [UEM – Scheduling Backup on page 228](#).

- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

13.7.3

UEM – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **uem01** application in the relevant zone, click **Run**.



NOTE: You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [UEM – Scheduling Backup on page 228](#).
- If you want to save the backup file on the NM Client PC, continue to [UEM – Downloading a Backup File to the NM Client PC on page 229](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

13.7.4

UEM – Scheduling Backup

Prerequisites: Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

a. In the **Name** field, type a name for the scheduled backup task.

b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **uem01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

c. In the **Day** drop-down list, select a week day or select **DAILY**.

d. In the **Hour** drop-down list, select at which hour the backup must run.

e. In the **Minute** drop-down list, select at which minute the backup must run.

f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [UEM – Downloading a Backup File to the NM Client PC on page 229](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

13.7.5

UEM – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `zone<XX>_uemdb_01_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[Unified Event Manager \(UEM\) – Software Application Restoration](#) on page 220

Chapter 14

Zone Database Server (ZDS) – Software Application Restoration

This table contains references to procedures to be performed to restore and back up the Zone Database Server (ZDS) application server. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 48: Zone Database Server – Restoration References

Action	Reference	Done
Software restoration	ZDS – Restoration Impact on page 231	
	ZDS – Pre-Restoration Checks on page 232	
	ZDS – Restoring Application on page 233	
	ZDS – Configuring Application on page 234	
	ZDS – Restoring Data from Backup on page 237	
	ZDS – Installing and Configuring RSA Authentication Software on page 240	
	ZDS – Post-Restoration Checks on page 240	
	ZDS – Backing Up Data on page 241	

14.1

ZDS – Restoration Impact

Table 49: ZDS – Restoration Impact

Action	Service Affected	Service Downtime
Database restoration	One ZDS is disabled to restore the database. Nationwide RCM data changes cannot be populated to this clusters ATR servers.	Approximately 1 hour for restoration from ZDS - depending on the size of database, server load, and network traffic.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration on page 231](#)

14.2

ZDS – Pre-Restoration Checks

Table 50: ZDS – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	<p>Check system IP Plan</p> <p>Multi-CADI</p> <p> NOTE: Multi-CADI still functions if UCS and ZDS are down, only new logons are not possible when the ZDS is down (required for restoring the UCS database).</p>
	<p>Check for READY/READY status of replication.</p>
	<p>Check trunking status and Security Class Status of BTS sites are at correct level before the ZDS restoration (if the security class restoration level is critical).</p>
	<p>Make sure that the ZDS application server is disabled prior to software restoration. Perform ZDS – Disabling Application Server on page 232.</p>

14.2.1

ZDS – Disabling Application Server

Prerequisites:

Log on to the server as `sysadmin` by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `sysadmin`, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Administration Menus**.

The list of installed Application Servers appears.

3. Enter the number associated with **Application Servers Status Administration**.
4. Enter the number associated with **Disable Application Servers**.
5. Enter the number associated with the application server that you want to disable.
6. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration](#) on page 231

14.3

ZDS – Restoring Software

14.3.1

ZDS – Restoring Application

Prerequisites: Log on to the server as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number associated with **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to re-install **Zone Database Server**, and enter: `n` for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering `q`
5. Log on to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number associated with **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number associated with **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number associated with **Zone Database Server**.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter: q and repeat this sequence until you log off from the server.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration](#) on page 231

14.3.2

ZDS – Configuring Application

The following describes how to properly configure the Zone Database Server (ZDS) application server.

14.3.2.1

ZDS – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.



IMPORTANT: Before enabling the ZDS application server, the database should be restored. For procedures, refer to [ZDS – Restoring Data from Backup](#) on page 237.

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q] :
```

2. Enter the number for **Application Servers Status Administration**.

3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

14.3.2.2

ZDS – Synchronizing Zone Database with UCS

Follow the procedure whenever synchronizing Zone Database with UCS is necessary, for example in case of the corruption of the Zone Database.

Prerequisites:

Disabling ZDS is required for this procedure. Disabling of the UCS and optimization of its database is recommended.

Log on to iGAS as sysadmin. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

The **Application Servers Administration Menus** appear.

3. Enter the number associated with the ZDS application server.

The login prompt appears.

4. Log on as dsadmin.

The application server displays initial administrative prompts.



NOTE: The initial administrative prompts vary depending on the application server in question.

5. Enter the number associated with **Database Administration**.

6. Enter the number associated with **Synchronize Zone Database with UCS**.



IMPORTANT: The ZDS must be disabled at this point.

The ZDS database is synchronized with UCS and a string of messages appears.

7. Enter: q until logged out of the application server and back to iGAS.

Postrequisites:

- Ensure the output does not communicate any errors. If you see error messages, contact your Motorola Solutions representative.
- Enable ZDS.

14.3.2.3

ZDS – Checking Data Replication Status

Data replication is the means used to ensure that the ZDS database has all the data contained in the UCS database. The **Check Data Replication Status** option on the UCS **Database Administration** menu may be used to check the status of data replication between ZDS and the UCS.



IMPORTANT: This procedure needs to be completed on both the UCS and ZDS.

Procedure:

1. On the **Application Servers Administration Menus** list, enter the number associated with **User Configuration Server Administration**.
The login prompt appears.
2. Log in as ucadmin.
The application server displays initial administrative prompts.
 **NOTE:** The initial administrative prompts vary depending on the application server in question.
3. Confirming by pressing **ENTER**, answer the application server's initial prompts.
You are logged on, and the **UCS Server Administration** menu appears.
4. Enter the number associated with **Database Administration**.
The **Database Administration** menu appears.
5. Enter the number associated with **Check Data Replication Status**.
The replication status between the UCS and the ZDS is displayed and the Database Administration menu then reappears.
6. Continue to check until the status **READY** from the UCS for the newly restored Zone Database Server zone is displayed. If no one changed the configuration on the UCS, status **READY** appears just after synch down, when both the ZDS and the UCS are enabled.
7. Enter: **q** until logged out back into iGAS.
8. On the **Application Servers Administration Menus** list, enter the number associated with **Zone Database Server Administration**.
The login prompt appears.
9. Log on as dsadmin.
The application server displays initial administrative prompts.
 **NOTE:** The initial administrative prompts vary depending on the application server in question.
10. Confirming by pressing **ENTER**, answer the application server's initial prompts.
You are logged on, and the **ZDS Server Administration** menu appears.

Zone Database Server Administration 1. Enable Zone Database Server 2. Enable Zone Database Server (fast) 3. Disable Zone Database Server 4. Display Server Status 5. Database Administration 6. Feature Administration 7. Unix Administration 8. Backup Server Administration 9. Multicloud Radio Control Manager Administration 10. ZDS Report Administration Enter Selection: (1-10, q) [q]:

11. Enter the number associated with **Database Administration**.

The Database Administration menu appears:

```
Database Administration 1. Optimize Database Administration 2. Export
Infrastructure Database 3. Set Up Automatic Infrastructure Database Export 4.
Check Data Replication Status 5. Check Outstanding Replications 6. Synchronize
Zone Database with UCS Enter Selection: (1-6, q) [q]:
```

12. Enter the number associated with **Check Data Replication Status**.

The replication status between the UCS and the ZDS is displayed and the **Database Administration** menu then reappears.

13. Continue to check until the status READY from the UCS for the newly restored Zone Database Server zone is displayed. If no one changed the configuration on the UCS, status READY appears just after synch down, when both the ZDS and the UCS are enabled.

14. Enter: q until logged out of the application server and back to iGAS.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration](#) on page 231

14.4

ZDS – Restoring Data from Backup

14.4.1

ZDS – Logging On to the Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the Options controlling SSH key exchange pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**

where **<Z0>** is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223**
where **<Z0>** is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:

- To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
- To connect without adding the server rsa2 key to the PuTTY cache, click **No**.

7. At the logon prompt, enter: `motorola`
8. At the prompt, enter the password.
9. Enter the number for the server you want to log on to.
10. At the logon prompt, enter: `sysadmin`
11. At the prompt, enter the current password.

The **System Administrator Main Menu** appears.

12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.
14. Log on as `dsadmin`

The server application's menu appears.

14.4.2

ZDS – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: `y`
A message appears showing that the application server is disabled.
5. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

14.4.3

ZDS – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.
A table appears, showing available backup files for applications in the different zones.
2. Click **Refresh File name**.
The file names of the backup files are read on the default storage for each application.
If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names

stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named zone<XX>_zdsdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

14.4.4

ZDS – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

14.4.5

ZDS – Verifying Zone Controller Redundancy

Prerequisites: You must be logged in to iGAS, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Type the number associated with **Application Servers Administration Menus**, and press ENTER.
2. Select the number associated with the **ZC Server** you want to configure and press ENTER.
The login prompt appears.
3. Log in as szadmin
The server application's menu appears.
4. Select the number associated with the **Zone Controller Administration**, and press ENTER.
5. Select the number associated with the **Redundancy Administration**, and press ENTER.
6. Select the number associated with the **Redundancy Information**, and press ENTER.
Information on redundancy appears.
7. Verify that **Requested Active ZC** and **Switchover Mode** are set according to your system configuration.

Postrequisites: Repeat this procedure for all Zone Controllers in the same Zone as ZDS.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration](#) on page 231

14.5

ZDS – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration](#) on page 231

14.6

ZDS – Post-Restoration Checks

Table 51: ZDS – Post-Restoration Checks

Action	Post-Restoration Checks
Software restoration	Check for READY/READY status of replication.

Action	Post-Restoration Checks
	Once the ZDS achieved READY/READY status, perform a SAC Download to the standby, and then the active ZC. See Downloading SAC to the ZCs on page 241 .
	Check if MTIG-IP server is working correctly. If ZDS restoration caused MTIG-IP NM configuration change, MTIG-IP reboot is required so that the change is applied. For more information on rebooting MTIG-IP server, see Rebooting the MTIG-IP Server on page 267 .

14.6.1

Downloading SAC to the ZCs

Procedure:

1. From the NM client, PRNM Suite, open the ZoneX folder.
2. Start the ZCM application.
3. In the ZCM application, find the **Zone Controller** object and the ZC02 instance (it should be active at the moment).
4. Right-click and choose **Diagnostics**.
5. Click on **SAC download**, and verify that it completes successfully.



NOTE: There might be a slight service disruption during that step, but it is very time limited.

6. Download SAC to all **ZCs**, for all zones.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration](#) on page 231

14.7

ZDS – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

14.7.1

ZDS – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

14.7.2

ZDS – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.
A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **zds01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the ZDS application in the correct zone.



NOTE: You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **zds01** application in the **Use Central Storage** column. Make sure that you select the check box for the ZDS in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **zds01** application in the **Use Storage PC** column.
5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [ZDS – Backing Up Data On-Demand on page 242](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [ZDS – Scheduling Backup on page 243](#).
- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

14.7.3

ZDS – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **zds01** application in the relevant zone, click **Run**.



NOTE: You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [ZDS – Scheduling Backup on page 243](#).
- If you want to save the backup file on the NM Client PC, continue to [ZDS – Downloading a Backup File to the NM Client PC on page 244](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

14.7.4

ZDS – Scheduling Backup

Prerequisites: Log on the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

- a. In the **Name** field, type a name for the scheduled backup task.
- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **zds01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.
- d. In the **Hour** drop-down list, select at which hour the backup must run.
- e. In the **Minute** drop-down list, select at which minute the backup must run.
- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [ZDS – Downloading a Backup File to the NM Client PC on page 244](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

14.7.5

ZDS – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `zone<XX>_zdsdb_01_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[Zone Database Server \(ZDS\) – Software Application Restoration on page 231](#)

Chapter 15

Zone Statistics Server (ZSS) – Software Application Restoration

This table contains references to procedures to be performed to restore and back up the Zone Statistics Server (ZSS) application server. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 52: Zone Statistics Server – Restoration References

Action	Reference	Done
Software restoration	ZSS – Restoration Impact on page 245	
	ZSS – Pre-Restoration Checks on page 245	
	ZSS – Restoring Application on page 247	
	ZSS – Configuring Application on page 248	
	ZSS – Restoring Data from Backup on page 249	
	ZSS – Installing and Configuring RSA Authentication Software on page 252	
	ZSS – Post-Restoration Checks on page 252	
	ZSS – Backing Up Data on page 252	

15.1

ZSS – Restoration Impact

Table 53: ZSS – Restoration Impact

Action	Service Affected	Service Downtime
Software restoration	ZSS unavailable – no zone historical reports kept for duration of restoration.	Approximately 2 hours.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration on page 245](#)

15.2

ZSS – Pre-Restoration Checks

Table 54: ZSS – Pre-Restoration Checks

Action	Pre-Restoration Checks
Software restoration	Take a new backup if the previous one is not available for use.

Action	Pre-Restoration Checks
	Check if the reported problem still exists.
	Check the Time Zone.
	Make sure that the application server is disabled prior to software restoration. Perform ZSS – Disabling the Application Server on page 246 .

15.2.1

ZSS – Disabling the Application Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**
where <Z0> is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223**
where <Z0> is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: **motorola**
8. At the prompt, enter the password.
9. Enter the number for **ZC/Unix Server Menu**.
10. Enter the number for the Core Server (Primary or Secondary) where the ZSS resides.
11. At the logon prompt, enter: **sysadmin**
12. At the prompt, enter the current password.
The **System Administrator Main Menu** appears.
13. Enter the number associated with **Application Servers Status Administration**.
14. Enter the number associated with **Disable Application Servers**.

15. Enter the number associated with the application server that you want to disable.
16. Enter **q** twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration](#) on page 245

15.3

ZSS – Restoring Software

15.3.1

ZSS – Restoring Application

Prerequisites: Ensure that the server is on.

Procedure:

1. On the NM Client PC, start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter: **10.<Z0>.233.222**

where **<Z0>** is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223**

where **<Z0>** is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: **motorola**
8. At the prompt, enter the password.
9. Select the option associated with the Core Server to which you want to log on.
10. At the logon prompt, enter: **instadm**
11. At the prompt, enter the current password.
The **Installation Administrator Main Menu** appears.
12. Enter the number for **Reinstall Applications**.

The list of available applications residing on the server appears.

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

13. Enter: **y** when the installer asks about reinstalling Zone Statistics Server, and type **n** for the other applications.

The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.

14. Enter: **q** to log off the server.

15. Log on to the server using the **sysadmin** login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

16. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

17. Enter the number for **Boot Application Servers**.

The **Boot Application** menu appears.

18. Enter the number for the Zone Statistics Server.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

19. Enter: **q** multiple times until you log off the server.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration on page 245](#)

15.3.2

ZSS – Configuring Application

15.3.2.1

ZSS – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration](#) on page 245

15.4

ZSS – Restoring Data from Backup

15.4.1

ZSS – Logging On to the Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the Options controlling SSH key exchange pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**

where <Z0> is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is

10.<Z0>.233.223

where <Z0> is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: **motorola**
8. At the prompt, enter the password.
9. Select the option associated with the **Primary Core Server** or **Secondary Core Server**.
10. At the logon prompt, enter: **sysadmin**
11. At the prompt, enter the current password.
The **System Administrator Main Menu** appears.
12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.
14. At the logon prompt, enter: **zssadmin**
The server application's menu appears.

15.4.2

ZSS – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: **y**
A message appears showing that the application server is disabled.
5. Enter **q** twice to go back to the **Application Servers Status Administration** menu.

15.4.3

ZSS – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.
A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.



NOTE: The backup file is named **zoneXX_zssdb_01_timestamp.tar.gz**, where XX is the zone ID, and timestamp is a date and time written as one row of digits with the format **yyyymmddhhmm**.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.



NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

15.4.4

ZSS – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. At logon as sysadmin, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.
3. Enter the number for **Enable Application Servers**.
4. Enter the number for the application server you want to enable.

A message appears showing that the application server is enabled.

5. Enter: q twice to go back to the **Application Servers Status Administration** menu.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration](#) on page 245

15.5

ZSS – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.



IMPORTANT: When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration](#) on page 245

15.6

ZSS – Post-Restoration Checks

Table 55: ZSS – Post-Restoration Checks

Action	Post-Restoration Tests
Software restoration	Check Zone Historical Reports.
	Run set of backups on all services.
	Check and clear Unified Event Manager alarms.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration](#) on page 245

15.7

ZSS – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

15.7.1

ZSS – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>

2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

15.7.2

ZSS – Configuring a Backup

Prerequisites:

Log on to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **zss01** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the ZSS application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **zss01** application in the **Use Central Storage** column. Make sure that you select the check box for the ZSS in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **zss01** application in the **Use Storage PC** column.
5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [ZSS – Backing Up Data On-Demand on page 253](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [ZSS – Scheduling Backup on page 254](#).
- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

15.7.3

ZSS – Backing Up Data On-Demand

Prerequisites:

Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **zss01** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows that the backup task has started, and it shows when the task has completed. The backup file is created on the local storage of the application, then transferred to the Zone UIS. If the **Use Central Storage** option was chosen, then it will be transferred to central storage. If the **Use Central Storage** and **Use Storage PC** option were chosen, then it will be transferred to Storage PC as well. If a backup file for the application already exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backups are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [ZSS – Scheduling Backup on page 254](#).
- If you want to save the backup file on the NM Client PC, continue to [ZSS – Downloading a Backup File to the NM Client PC on page 255](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

15.7.4

ZSS – Scheduling Backup

Prerequisites: Log on to the Upgrade Console on the Master UIS, with the **Backup** user role. Configure the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Perform the following actions:
 - a. In the **Name** field, type a name for the scheduled backup task.
 - b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.
A list appears in which you must click **Select** in the row containing the **zss01** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.
 - c. In the **Day** drop-down list, select a week day or select **DAILY**.

- d. In the **Hour** drop-down list, select at which hour the backup must run.
- e. In the **Minute** drop-down list, select at which minute the backup must run.
- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites: If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [ZSS – Downloading a Backup File to the NM Client PC on page 255](#). Otherwise, you do not have to do anything else regarding backup.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

15.7.5

ZSS – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Log on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Download Files**.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `zoneXX_zssdb_01_timestamp.tar.gz`, where XX is the zone ID, and timestamp is a date and time written as one row of digits with the format `yyyymmddhhmm`.

 **NOTE:** You can only download one file at a time.

A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[Zone Statistics Server \(ZSS\) – Software Application Restoration on page 245](#)

Chapter 16

MTIG-IP Restoration

The following describes the backup and restoration procedures involved with the elements of the Motorola Telephone Interconnect Gateway using SIP signaling towards the PABX. This Motorola Telephone Interconnect Gateway is called MTIG-IP.

This table contains references to procedures to be performed to restore and back up the MTIG-IP application server software. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 56: MTIG-IP – Backup and Restoration Checklist

Action	Reference	Done
Restoring the application	MTIG-IP – Restoration Impact on page 256	
	MTIG-IP – Pre-Restoration Checks on page 256	
	MTIG-IP – Restoring Software on page 257	
	MTIG-IP – Restoring Data from Backup on page 259	
	MTIG-IP – Installing and Configuring RSA Authentication Software on page 263	
	MTIG-IP – Post-Restoration Checks on page 263	
Backing up the application	MTIG-IP – Backing Up Data on page 263	

16.1

MTIG-IP – Restoration Impact

Table 57: MTIG-IP – Restoration Impact

Action	Service Affected	Service Downtime
MTIG-IP restoration	MTIG-IP services are unavailable to the radio system. Therefore, schedule the restoration to periods when overall service is influenced the least. Local added tones are restored (if they were backed up), but changed default tones are lost.	

16.2

MTIG-IP – Pre-Restoration Checks

Before you do any restoration tasks, make sure that you are familiar with the guidelines described in the *Safety Guidelines for Installation of Hardware and Software* manual.

16.3

MTIG-IP – Restoring Software

16.3.1

MTIG-IP – Restoring Application

Prerequisites:

Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Type the number associated with **Reinstall Applications** and press **Enter**.

The list of available applications residing on the server appears.

3. Type **y** when the installer asks about reinstalling MTIG-IP and type **n** for the other applications.

The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.

4. Type **q** to log off the server.

5. Log in to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Type the number associated with **Application Servers Boot/Reboot/Shutdown** and press **Enter**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Type the number associated with **Boot Application Servers** and press **Enter**.

The **Boot Application** menu appears.

8. Type the number associated with MTIG-IP and press **Enter**.

You have rebooted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter **q** and press **Enter**. Repeat this sequence until you log off the server.

Related Links

[MTIG-IP – Configuring Application](#) on page 258

16.3.2

MTIG-IP – Configuring Application

Related Links

[MTIG-IP – Restoring Application](#) on page 257

16.3.2.1

Configuring the Host Based Firewall Rules

Prerequisites:

Log on to iGAS as **sysadmin**. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server](#) on page 45
- [Logging On to iGAS Through a KVM Switch](#) on page 48

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

The Application Servers Administration Menus appear.

3. Enter the number associated with **Motorola Telephone Interconnect Gateway**.

A logon prompt appears.

4. Log on as **fwadmin**.

The Firewall administration menu appears.

```
Firewall administration menu ----- 1. Display firewall
status 2. View operational (OP) rule set 3. View non-operational (NOP) rule set
4. Check out the NOP rule set 5. Copy OP rule set to the NOP rule set 6. Edit NOP
rule set 7. Check in the NOP rule set 8. Activate new rule set (exchange OP<->NOP)
9. Change password Please enter selection (1-9, q) [q]:
```

5. Enter the number associated with **Check out the NOP rule set**.

The following message appears:

The file has been checked out successfully.

6. Enter the number associated with **Copy OP rule set to the NOP rule set**.

The following message appears:

OP file copied to the NOP file successfully.

7. Enter the number associated with **Edit NOP rule set**.



NOTE: The firewall rules use the Linux iptables syntax.

The contents of the NOP rule set are displayed. The following messages are an example from the set for PABX:

```
[BLOCK_PABX] - A INPUT -s 192.168.2.0/24 -p tcp --dport 5060 -j ACCEPT - A OUTPUT  
-s 192.168.2.0/24 -p tcp --dport 5060 -j ACCEPT - A INPUT -s 192.168.2.0/24 -p  
udp --dport 1024:65535 -j ACCEPT - A OUTPUT -s 192.168.2.0/24 -p udp --dport  
1024:65535 -j ACCEPT [BLOCK_ALL] - A INPUT -i eth1 -j DROP - A OUTPUT -i eth1  
-j DROP
```

8. Modify the rule according to your needs. For the PABX scenario, the possible change could be to allow an extra set of IP addresses in case the PABX have more than one IP address.



NOTE: The editor supports VI commands.

9. Enter the number associated with **Check in the NOP rule set**.

The following message appears:

The file has been checked in.

10. When done, enter the number associated with **Activate new rule set (exchange OP<->NOP)**.

The following message appears:

```
iptables: Saving firewall rules to /etc/sysconfig/iptables: [ OK ] New firewall  
rules activated successfully.
```

Related Links

[MTIG-IP Restoration](#) on page 256

16.4

MTIG-IP – Restoring Data from Backup

16.4.1

MTIG-IP – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>

 **IMPORTANT:**

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.

3. In the **Password** field, type the password related to the user name.

4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [MTIG-IP – Uploading a Backup File to UIS on page 260](#). If the backup file already is in the UIS backup storage, continue to [MTIG-IP – Logging On to the Server on page 261](#).

16.4.2

MTIG-IP – Uploading a Backup File to UIS

Prerequisites: You must be logged in to the Upgrade Console with the **Backup** user role. A data backup file must be available on the NM Client PC from where you have launched the Upgrade Console. You want to upload this backup file to the UIS backup storage, so that you can use it for restoration of data.

 **NOTE:** If you already have stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. Select **Upload Files** in the menu at the left side of the Upgrade Console.

The **Upload Files** page appears.

2. Click **Browse**.

3. Select the relevant backup file in the window that appears, and click **OK**.

 **NOTE:** The backup file is named zone<XX>_mtigipdb_01-02_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

The file is uploaded to a “drop zone”, where the uploaded files are placed temporarily.

5. Click **Analyze Uploaded File** to check the file in the drop zone.

If the file format is correct, the file is placed in the backup storage of the UIS, you are connected to. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

16.4.3

MTIG-IP – Logging On to the Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the Options controlling SSH key exchange pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**

where **<Z0>** is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is **10.<Z0>.233.223** where **<Z0>** is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: **motorola**
8. At the prompt, enter the password.
9. Enter the number for **MTIG-IP Server**.
10. At the logon prompt, enter: **sysadmin**
11. At the prompt, enter the current password.

The **System Administrator Main Menu** appears.

12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.

16.4.4

MTIG-IP – Disabling the Application Server

Prerequisites:

Before you start this procedure, you must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Type the number associated with **Application Servers Status Administration**, and press **Enter**.

2. Type the number associated with **Disable Application Servers**, and press **Enter**.
3. Type the number associated with the application server that you want to disable, and press **Enter**.
A message appears showing that the application server is disabled.
4. Type **q** twice to go back to the **Application Servers Status Administration** menu.

16.4.5

MTIG-IP – Restoring Data from Backup

Prerequisites: You must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. Select **Restore** in the menu at the left side of the Upgrade Console.
A table appears showing available backup files for applications in the different zones.
2. Click **Refresh filename**.
The file names of the backup files are read on the default storage for each application. If you configured the usage of central storage for the backup, the default storage is Master UIS. Otherwise, it is Zone UIS. If you configured a Storage PC then a list of backup file names stored on Storage PCs will be available.
3. Select **Backup Filename** and from the drop-down list, choose the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.
The backup file is named `zone<XX>_mtigipdb_01-02_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.
A message appears asking whether you are sure that you want to restore data.
5. Click **Yes**.
An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has completed.
 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

16.4.6

MTIG-IP – Enabling the Application Server

Prerequisites:

Before you start this procedure, you must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Type the number associated with **Application Servers Status Administration**, and press **Enter**.
2. Type the number associated with **Enable Application Servers**, and press **Enter**.

3. Type the number associated with the application server you want to enable, and press **Enter**.
A message appears showing that the application server is enabled.
4. Type **q** twice to go back to the **Application Servers Status Administration** menu.

16.5

MTIG-IP – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

16.6

MTIG-IP – Post-Restoration Checks

Restart the application to check that it is working.

16.7

MTIG-IP – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

16.7.1

MTIG-IP – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>



IMPORTANT:

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.
3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [MTIG-IP – Uploading a Backup File to UIS on page 260](#). If the backup file already is in the UIS backup storage, continue to [MTIG-IP – Logging On to the Server on page 261](#).

16.7.2

MTIG-IP – Configuring a Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.
A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.
2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **mtig_ip01** or **mtig_ip02** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the MTIG-IP application in the correct zone.
 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.
3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **mtig_ip01** or **mtig_ip02** application in the **Use Central Storage** column. Make sure that you select the check box for the MTIG-IP in the correct zone.
4. If you want to save the backup file in the Storage PC, select the check box of the **mtig_ip01** or **mtig_ip02** application in the **Use Storage PC** column.
 **NOTE:** The backup file will be saved on all Storage PCs.
5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [MTIG-IP – Backing Up Data On-Demand on page 265](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [MTIG-IP – Scheduling Backup on page 265](#).
- You can do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

16.7.3

MTIG-IP – Backing Up Data On-Demand

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **mtig_ip01** or **mtig_ip02** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites: You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [MTIG-IP – Scheduling Backup on page 265](#).
- If you want to save the backup file on the NM Client PC, continue to [MTIG-IP – Downloading a Backup File to the NM Client PC on page 266](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do any further regarding backup.

16.7.4

MTIG-IP – Scheduling Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Do the following:
 - a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **mtig_ip01** or **mtig_ip02** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.
- d. In the **Hour** drop-down list, select at which hour the backup must run.
- e. In the **Minute** drop-down list, select at which minute the backup must run.
- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

- 4. If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [MTIG-IP – Downloading a Backup File to the NM Client PC on page 266](#). Otherwise, you do not have to do anything further regarding backup.

Postrequisites:

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

16.7.5

MTIG-IP – Downloading a Backup File to the NM Client PC

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named `zone<XX>_mtigipdb_01-02_<timestamp>.tar.gz`, where `<XX>` is the zone ID, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

 **NOTE:** You can only download one file at a time.

A warning appears asking whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

16.8

Rebooting the MTIG-IP Server

Procedure:

1. Log on to the server using the **sysadmin** login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Type the number associated with **Application Servers Boot/Reboot/Shutdown** and press **Enter**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown
-----
1. Boot Application Servers
2. Reboot Application Servers
3. Shutdown Application Servers
Please enter selection (1-3, q) [q]:
```

3. Type the number associated with **Reboot Application Servers** and press **Enter**.

The **Boot Application** menu appears.

4. Type the number associated with **MTIG-IP Server** and press **Enter**.

The MTIG-IP Server application residing on the server reboots.

Chapter 17

Data Subsystem Restoration

17.1

Packet Data Gateway (PDG) – Software Application Restoration

The following sections describe the backup and restoration procedures involved with the elements of the Packet Data Gateway. This Packet Data Gateway is called PDG.

The PDG comprises Packet Data Router (PDR) and Radio Network Gateway (RNG), and is logically considered as one unit. Physically, the PDR and RNG are separate application servers located on one physical server. Data backup and restoration are performed on the PDR only.

17.1.1

PDG – Restoration References

This table contains references to procedures to be performed to restore and back up the PDR application server software. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 58: PDG – Restoration References

Action	Reference	Done
Restoring the application	PDG – Restoration Impact on page 269	
	PDG – Pre-Restoration Checks on page 269	
	PDG – Restoring Software on page 269	
	PDG – Configuring Application on page 271	
	PDG – Restoring Data from Backup on page 271	
	PDG – Installing and Configuring RSA Authentication Software on page 274	
	PDG – Post-Restoration Checks on page 274	
Backing up the application	PDG – Backing Up Data on page 277	

17.1.2

PDG – Restoration Impact

Table 59: PDG – Restoration Impact

Action	Service Affected	Service Downtime
All PDG restoration procedures	PDG services are unavailable to the radio system. Therefore, schedule the restoration to periods when overall service is influenced the least.	

17.1.3

PDG – Pre-Restoration Checks

Before you do any restoration tasks, make sure that you are familiar with the guidelines described in the *Safety Guidelines for Installation of Hardware and Software* manual.

Related Links

[PDG – Restoration References](#) on page 268

17.1.4

PDG – Restoring Software

17.1.4.1

PDR – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Type the number associated with **Reinstall Applications** and press **Enter**.
The list of available applications residing on the server appears.
3. Enter: `y` when the installer asks about reinstalling PDR and enter: `n` for the other applications.
The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.
4. Enter: `q` to log off the server.
5. Log on to iGAS as `sysadmin`
The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number for **Boot Application Servers**.

8. Enter the number associated with PDR.

You have booted the application.

9. Enter: q repeatedly until you log off the server.

17.1.4.2

RNG – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Type the number associated with **Reinstall Applications** and press **Enter**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer asks about reinstalling RNG and enter: `n` for the other applications.

The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.

4. Enter: `q` to log off the server.

5. Log on to iGAS as `sysadmin`

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
```

```
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number for **Boot Application Servers**.

8. Enter the number associated with RNG.

You have booted the application.

9. Enter: q repeatedly until you log off the server.

Related Links

[PDG – Restoration References](#) on page 268

17.1.5

PDG – Configuring Application

The procedure works for redundant and non-redundant deployments.

After the introduction of the SRS framework, Packet Data Gateway (as well as Short Data Router – SDR) is automatically switched to the correct state, depending on peer state. If the peer is available and active, it will follow the state of the adjacent peer and enter standby mode. If the peer is not available, it will try to activate itself.

However, booted right after the installation, the application enters maintenance state. You can configure the PDG to enable automatic switchovers by performing this procedure.

Procedure:

1. Enable the primary PDG. See [Enabling the Application Server on page 66](#).
2. Wait a minute and enable the secondary PDG. See [Enabling the Application Server on page 66](#).

Related Links

[PDG – Restoration References](#) on page 268

17.1.6

PDG – Restoring Data from Backup

17.1.6.1

PDG – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>

 **IMPORTANT:**

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.

3. In the **Password** field, type the password related to the user name.

4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [PDG – Uploading a Backup File to UIS on page 272](#). If the backup file already is in the UIS backup storage, continue to [PDG – Logging On to the Server on page 272](#).

17.1.6.2

PDG – Uploading a Backup File to UIS

 **NOTE:** If you already have stored the required backup file in the UIS backup storage, you can skip this procedure.

Prerequisites: You must be logged in to the Upgrade Console with the **Backup** user role. A data backup file must be available on the NM Client PC from where you have launched the Upgrade Console. You want to upload this backup file to the UIS backup storage, so that you can use it for restoration of data.

Procedure:

1. Select **Upload Files** in the menu at the left side of the Upgrade Console.

The **Upload Files** page appears.

2. Click **Browse**.

3. Select the relevant backup file in the window that appears, and click **OK**.

 **NOTE:** The backup file is named zone<XX>_pdrdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

The file is uploaded to a “drop zone”, where the uploaded files are placed temporarily.

17.1.6.3

PDG – Logging On to the Server

Prerequisites: Ensure that the server is on.

Procedure:

1. Start PuTTY.
2. In the PuTTY Configuration window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the Options controlling SSH key exchange pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter **10.<Z0>.233.222**
where **<Z0>** is the zone octet where the terminal server is located.



NOTE:

For systems with Geographical Redundancy the IP address of the terminal server in location B is
10.<Z0>.233.223
where **<Z0>** is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: **motorola**
8. At the prompt, enter the password.
9. Enter the number for the server you want to log on to.
10. At the logon prompt, enter: **sysadmin**
11. At the prompt, enter the current password.
The **System Administrator Main Menu** appears.
12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.

17.1.6.4

PDG – Restoring Data from Backup

Prerequisites:

- You must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role.
- A data backup file must be available and the restoration should be performed in enabled state.

Procedure:

1. Select **Restore** in the menu at the left side of the Upgrade Console.



NOTE: The backup file will only appear in the table if a backup has been configured for the application server. For more information, see [PDG – Configuring a Backup on page 277](#) and [PDG – Scheduling Backup on page 279](#).

A table appears showing available backup files for applications in the different zones.

2. Click **Refresh filename**.

The file names of the backup files are read on the default storage for each application. If you configured the usage of central storage for the backup, the default storage is Master UIS. Otherwise, it is Zone UIS. If you configured a Storage PC then a list of backup file names stored on Storage PCs will be available.

3. Select **Backup Filename** and from the drop-down list, choose the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named zone<XX>_pdrdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

5. Click **Yes**.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has completed.

17.1.7

PDG – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[PDG – Restoration References](#) on page 268

17.1.8

PDG – Post-Restoration Checks

Table 60: PDG – Post-Restoration Checks

Action	Post-Restoration Checks
PDG	<p>Test data services – send a file: host to radio, radio to host.</p> <p>Check the synchronization status. See PDG – Checking Database Synchronization on page 275.</p> <p>Check the status of the network and devices in UEM.</p>

Action	Post-Restoration Checks
	<p>Perform the following actions:</p> <p> NOTE: The Local Configuration Main Menu must be open before performing these checks. See PDG – Checking Database Synchronization on page 275 for how to start the configuration interface.</p> <ul style="list-style-type: none">● Select Local RNG Link Status.● Check the Sites show Connected and all relevant sites are present.● Select Back to Start page.● Press q.● Press y to confirm quit and press enter.● At the pdr_mgr prompt, type <code>cat /etc/hosts</code> and check that all of the APN names show with a prefix of the Data Subsystem name configured in the UCM Data System Object and are mapped to the correct GGSN IP Address.● Type <code>exit</code> and press enter to logout of the PDR.
	<p>Check Packet Data Functionality:</p> <ul style="list-style-type: none">● Connect a Radio configured for PD with a suitable APN assigned to it and to a PC.● Connect / Context Activate the Radio from the PC.● When context is activated, test:<ul style="list-style-type: none">○ File transfer or relevant application to another radio using the same APN.○ File transfer or relevant application to a fixed host which is configured to be linked to the same APN.

17.1.8.1

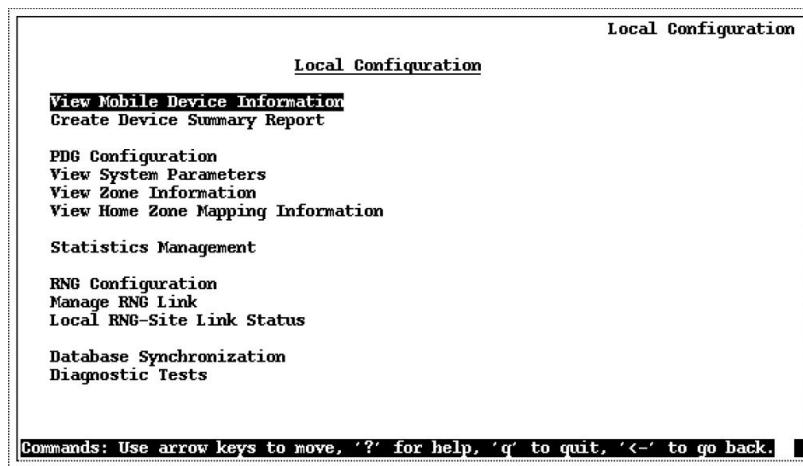
PDG – Checking Database Synchronization

Procedure:

1. Log on to the PDR as pdr_mgr.
2. Type `pwd` and press **Enter** to verify that your current directory is the PDR executable directory: `/home/pdr/bin`. If necessary, type `cd /home/pdr/bin` at the prompt and press **Enter** to move to the executable directory.
3. At the `[pdr_mgr@pdr01 bin]$` prompt, type `config` and press **Enter**.

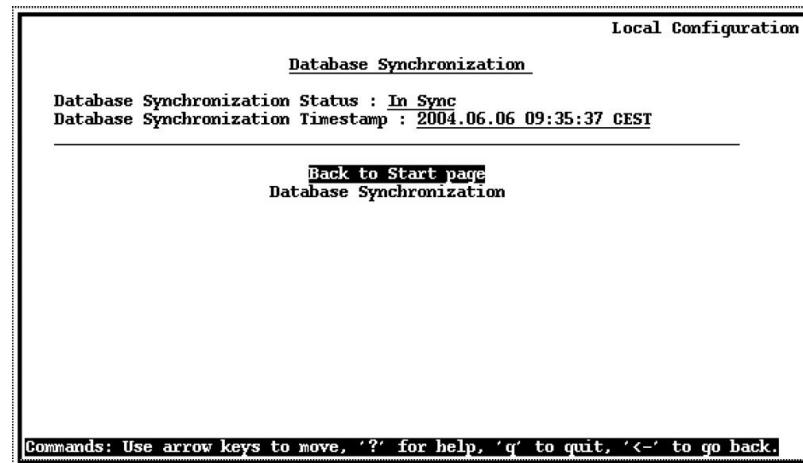
The PDR Local Configuration menu is displayed.

Figure 12: PDR – Local Configuration Main Menu



4. Use the arrow keys to select **Database Synchronization** from the Configuration menu.
5. Press **Enter**.
The Database Synchronization screen is displayed.
6. To view the Database Synchronization status, use the arrow keys to highlight **View Database Synchronization Status**, and press **Enter** (see below for an example).

Figure 13: PDR – Database Synchronization Screen



7. To Initiate Database Synchronization, use the arrow keys to highlight **Initiate Database Synchronization**, and press **Enter**.
8. To see the result, use the arrow keys to highlight **REFRESH STATUS**, and press **Enter**.

17.1.8.2

PDR – Checking Synchronization Between the Active PDR and the Standby PDR

Prerequisites: Before the switchover, verify the current device status. If the UEM client is not running, see the "Starting the UEM Client" procedure in the *Unified Event Manager* manual.

Procedure:

Ensure that the Synchronization State on PDG is set to SYNCHRONIZED. See "Viewing Redundancy Information of a Device" in the *Unified Event Manager* manual.

 **NOTE:** Some configuration and state/data changes may require up to 5 minutes to completely synchronize to the standby PDG.

Related Links

[PDG – Restoration References](#) on page 268

17.1.9

PDG – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

17.1.9.1

PDG – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>



IMPORTANT:

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.
3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

17.1.9.2

PDG – Configuring a Backup

Prerequisites: You must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **active_pdr** application in the **Add To Backup/Restore** column. Ensure that you select the check box for the PDG application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **active_pdr** application in the **Use Central Storage** column. Ensure that you select the check box for the PDR in the correct zone.

4. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [PDR – Backing up Data On-Demand on page 278](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [PDG – Scheduling Backup on page 279](#).
- You can also do both.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

17.1.9.3

PDR – Backing up Data On-Demand

Prerequisites: You must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
- The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **active_pdr** application in the relevant zone, click **Run**.

 **NOTE:**

You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

When the backup task is initiated, the Enhanced Software Update tool finds out whether any of the redundant applications are active. If there is an active application, the backup is performed for this application. If none of the redundant applications are active, the backup fails.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites: You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [PDG – Scheduling Backup on page 279](#).
- If you want to save the backup file on the NM Client PC, continue to [PDG – Downloading a Backup File to the NM Client PC on page 280](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

17.1.9.4

PDG – Scheduling Backup

Prerequisites: You must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Perform the following actions:

- a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **active_pdr** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.

- d. In the **Hour** drop-down list, select at which hour the backup must run.

- e. In the **Minute** drop-down list, select at which minute the backup must run.

- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

4. If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [PDG – Downloading a Backup File to the NM Client PC on page 280](#). Otherwise, you do not have to do anything else regarding backup.

Postrequisites:



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

17.1.9.5

PDG – Downloading a Backup File to the NM Client PC

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

You must be logged in to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named zone<XX>_pdrrdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

 **NOTE:** You can only download one file at a time.

A warning appears asking whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[PDG – Restoration References](#) on page 268

17.2

Short Data Router (SDR) – Software Application Restoration

The following sections describe the backup and restoration procedures involved with the elements of the Short Data Router (SDR).

17.2.1

SDR – Restoration References

This table contains references to procedures to be performed to restore and back up the SDR application server software. Perform the procedures in the order specified in the table. You can use the last column to insert a check mark when a given procedure has been performed.

Table 61: SDR – Restoration References

Action	Reference	Done
Restoring the application	SDR – Restoration Impact on page 281 SDR – Pre-Restoration Checks on page 281 SDR – Restoring Software on page 281 SDR – Configuring Application on page 282 SDR – Restoring Data from Backup on page 285 SDR – Installing and Configuring RSA Authentication Software on page 285 SDR – Post-Restoration Checks on page 286	
Backing up the application	SDR – Backing Up Data on page 287	

17.2.2

SDR – Restoration Impact

Table 62: SDR – Restoration Impact

Action	Service Affected	Service Downtime
All SDR restoration procedures	SDR services are unavailable to the radio system. Therefore, schedule the restoration to periods when overall service is influenced the least.	

17.2.3

SDR – Pre-Restoration Checks

Before you do any restoration tasks, make sure that you are familiar with the guidelines described in the *Safety Guidelines for Installation of Hardware and Software* manual.

Related Links

[SDR – Restoration References on page 280](#)

17.2.4

SDR – Restoring Software

17.2.4.1

SDR – Restoring Application

Prerequisites: Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Type the number associated with **Reinstall Applications** and press **Enter**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer asks about reinstalling SDR and enter: `n` for other applications.

The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.

4. Enter: `q` to log off the server.

5. Log on to iGAS as `sysadmin`

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number for **Boot Application Servers**.

8. Enter the number associated with SDR.

You have booted the application.

9. Enter: `q` repeatedly until you log off the server.

Related Links

[SDR – Restoration References](#) on page 280

17.2.5**SDR – Configuring Application**

The procedure works for redundant and non-redundant deployments.

After the introduction of the SRS framework, Short Data Router (as well as Packet Data Gateway – PDG) is automatically switched to the correct state, depending on peer state. If the peer is available and active, it will follow the state of the adjacent peer and enter standby mode. If the peer is not available, it will try to activate itself.

However, booted right after the installation, the application enters maintenance state. You can configure the SDR to enable automatic switchovers by performing this procedure.

Procedure:

1. Enable the primary SDR. See [Enabling the Application Server on page 66](#).
2. Wait a minute and enable the secondary SDR. See [Enabling the Application Server on page 66](#).

Related Links

[SDR – Restoration References](#) on page 280

17.2.6

SDR – Restoring Data from Backup

17.2.6.1

SDR – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>



IMPORTANT:

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.
3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [SDR – Uploading a Backup File to UIS on page 283](#). If the backup file already is in the UIS backup storage, continue to [SDR – Logging On to the Server on page 284](#).

17.2.6.2

SDR – Uploading a Backup File to UIS



NOTE: If you already have stored the required backup file in the UIS backup storage, you can skip this procedure.

Prerequisites: You must be logged in to the Upgrade Console with the **Backup** user role. A data backup file must be available on the NM Client PC from where you have launched the Upgrade Console. You want to upload this backup file to the UIS backup storage, so that you can use it for restoration of data.

Procedure:

1. Select **Upload Files** in the menu at the left side of the Upgrade Console.

The **Upload Files** page appears.

2. Click **Browse**.

3. Select the relevant backup file in the window that appears, and click **OK**.

 **NOTE:** The backup file is named zone<XX>_sdrdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

The file is uploaded to a “drop zone”, where the uploaded files are placed temporarily.

17.2.6.3

SDR – Logging On to the Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter 10.<Z0>.233.222

where <Z0> is the zone octet where the terminal server is located.

 **NOTE:**

For systems with Geographical Redundancy the IP address of the terminal server in location B is 10.<Z0>.233.223

where <Z0> is the zone octet.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: motorola
8. At the prompt, enter the password.
9. Select the option associated with the **Primary Core Server** or **Secondary Core Server** to which you want to log on.
10. At the login prompt, enter: consu

11. At the prompt, enter the current password.

17.2.6.4

SDR – Restoring Data from Backup

Prerequisites:

Log on to the Upgrade Console on the Master UIS with the **Backup** user role.

Ensure that a data backup file is available.

Procedure:

1. Select **Restore** in the menu at the left side of the Upgrade Console.

A table appears showing available backup files for applications in the different zones.

 **NOTE:** The backup file will only appear in the table if a backup has been configured for the application server. For more information, see [SDR – Configuring a Backup on page 287](#) and [SDR – Scheduling Backup on page 289](#).

2. Click **Refresh filename**.

The file names of the backup files are read on the default storage for each application. If you configured the usage of central storage for the backup, the default storage is Master UIS. Otherwise, it is Zone UIS. If you configured a Storage PC then a list of backup file names stored on Storage PCs will be available.

3. Select **Backup Filename** and from the drop-down list, choose the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named zone<XX>_sdrdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyyymmddhhmm>.

A message appears asking whether you are sure that you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has completed.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

17.2.7

SDR – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.

2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see "Installing and Configuring the RSA Authentication on Linux Devices" in the *Network Security* manual.



IMPORTANT: When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

Related Links

[SDR – Restoration References](#) on page 280

17.2.8

SDR – Post-Restoration Checks

Table 63: SDR – Post-Restoration Checks

Action	Post-Restoration Checks
SDR	<p>Test Short Data Services - send a message: host to radio, radio to radio, radio to host.</p> <p>Check the synchronization status. See SDR – Checking SDR Database Synchronization on page 286.</p> <p>Check the status of the network and devices in UEM.</p>

17.2.8.1

SDR – Checking SDR Database Synchronization

Procedure:

1. Log in to the SDR as **sdr_mgr**.
2. In case of a redundant SDR, ensure that this is the active server by running the command `srs_status`.
3. To start the configuration interface, enter `config`
4. Enter the number associated with **Data Distribution Interface**.
5. Enter the number associated with **View/Modify DDI Server**.
6. From the menu, select the **UCS** server and check if the UCS synchronization has finished:

```
Started
Finished
Full sync :
02/09/16 16:16:00
02/09/16 16:16:03 Completed
```

7. From the menu, select the **ZDS** server and verify that the ZDS synchronization has finished.
8. In case UCS or ZDS synchronization has not finished, from the **Data Distribution Interface** menu, select the appropriate **Synchronize to <server name>** entry.

17.2.8.2

SDR – Verifying the Active-Standby SDR Synchronization

Prerequisites: Before the switchover, verify the current device status. If the UEM client is not running, follow the "Starting the UEM Client" procedure in the *Unified Event Manager* manual.

Procedure:

Ensure that the Synchronization State on SDR is set to SYNCHRONIZED. See "Viewing Redundancy Information of a Device" in the *Unified Event Manager* manual.

 **NOTE:** Some configuration and state/data changes may require up to 5 minutes to completely synchronize to the standby SDR.

Related Links

[SDR – Restoration References](#) on page 280

17.2.9

SDR – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

17.2.9.1

SDR – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>



IMPORTANT:

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.
3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

17.2.9.2

SDR – Configuring a Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **active_sdr** application in the **Add To Backup/Restore** column. Ensure that you select the check box for the SDR application in the correct zone.

 **NOTE:** You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **active_sdr** application in the **Use Central Storage** column. Ensure that you select the check box for the SDR in the correct zone.

4. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [SDR – Backing Up Data On-Demand on page 288](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [SDR – Scheduling Backup on page 289](#).
- You may also perform both of these actions.

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

17.2.9.3

SDR – Backing Up Data On-Demand

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.
- The **Backup** page appears showing applications selected for backup.
2. In the **Action** column of the **active_sdr** application in the relevant zone, click **Run**.

 **NOTE:**

You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

When the backup task is initiated, the Enhanced Software Update tool finds out whether any of the redundant applications are active. If there is an active application, the backup is performed for this application. If none of the redundant applications are active, the backup fails.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [SDR – Scheduling Backup on page 289](#).
- If you want to save the backup file on the NM Client PC, continue to [SDR – Downloading a Backup File to the NM Client PC on page 290](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

17.2.9.4

SDR – Scheduling Backup

Prerequisites: Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have configured the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Do the following:

- a. In the **Name** field, enter a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **active_sdr** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.

- d. In the **Hour** drop-down list, select at which hour the backup must run.

- e. In the **Minute** drop-down list, select at which minute the backup must run.

- f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

4. If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [SDR – Downloading a Backup File to the NM Client PC on page 290](#). Otherwise, you do not have to do anything else regarding backup.

Postrequisites:



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

17.2.9.5

SDR – Downloading a Backup File to the NM Client PC

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.

 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

 **NOTE:** The backup file is named zone<XX>_sdrdb_01_<timestamp>.tar.gz, where <XX> is the zone ID, and <timestamp> is a date and time written as one row of digits with the format <yyyymmddhhmm>.

 **NOTE:** You can only download one file at a time.

A warning appears asking whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.

Related Links

[SDR – Restoration References](#) on page 280

Chapter 18

MCC 7500 Dispatch Communications Server (DCS) Subsystem Restoration

Topic paragraph

18.1

Audio Gateway (AGTW) Software Application Restoration

Table 64: Audio Gateway (AGTW) Server – Backup and Restoration Checklist

Action	Reference	Done
Restoring the application	AGTW – Restoration Impact on page 291	
	AGTW – Pre-Restoration Checks on page 291	
	AGTW – Restoring Application on page 292	
	AGTW – Application Configuration on page 293	
	AGTW – Restoring Data from Backup on page 293	
	AGTW – Installing and Configuring RSA Authentication Software on page 297	
	AGTW – Post-Restoration Checks on page 297	
Backing up the application	AGTW – Backing Up Data on page 297	

18.1.1

AGTW – Restoration Impact

Table 65: AGTW – Restoration Impact

Action	Service Affected	Service Downtime
Stop the AGTW Service	No audio is processed, while the AGTW Service is stopped. All ongoing calls are stopped. All connections to the CCE Server are broken.	

18.1.2

AGTW – Pre-Restoration Checks

While the Audio Gateway (AGTW) Server is restored all calls are stopped and no audio is processed. Make sure to stop all ongoing calls prior to starting the restoration.

No additional pre-restoration checks need to be performed.

18.1.3

AGTW – Restoring Software

18.1.3.1

AGTW – Restoring Application

Prerequisites:

Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu ----- 1.
Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to reinstall the **Audio Gateway Server** and enter: `n` for the other applications.

The reinstallation process starts. When the reinstallation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering: `q`

5. Log on to the server using the `sysadmin` login and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number for **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number for **Audio Gateway Server**.

You have booted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter: q and repeat this sequence until you log off from the server.

18.1.3.2

AGTW – Application Configuration

Once the AGTW Server is installed it is ready to operate. No additional configuration of the AGTW Server software is needed.

The AGTW Server is an Application Server installed on the MCC 7500 Dispatch Communications Server (DCS). For the MCC 7500 DCS to be fully operational:

- Both the Call Control Entity (CCE) Server and the Audio Gateway (AGTW) Server applications need to be installed on the MCC 7500 DCS.
- The DCS needs to be configured in the Zone Configuration Manager (ZCM) application.

For more details on backup and restore procedures for the CCE Server, see [Call Control Entity \(CCE\) Software Application Restoration on page 301](#).

The configuration of the MCC 7500 DCS in the Zone Configuration Manager (ZCM) application includes the following objects:

- Dispatch Communications Server Application object
- Speaker Channel object

For details on configuring these objects, see the *Zone Configuration Manager* manual.

18.1.4

AGTW – Restoring Data from Backup

18.1.4.1

AGTW – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [AGTW – Uploading a Backup File to UIS on page 294](#). If the backup file already is in the UIS backup storage, continue to [AGTW – Logging On to the Server on page 294](#).

18.1.4.2

AGTW – Uploading a Backup File to UIS

Prerequisites: Log on to the Upgrade Console with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the Upgrade Console.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.

 **NOTE:** If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Upload Files**.

The **Upload Files** screen appears.

2. Click **Browse**.

3. Select the relevant backup file in the window that appears, and click **OK**.

 **NOTE:** The backup file is named `zone<XX>.nmd<YY>_agtwdb_<ZZ>_<timestamp>`, where `<XX>` is the zone ID, `<ZZ>` is a number in the interval 01-05, `<YY>` is a number in the interval 1-230, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyymmddhhmm>`.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

5. Click **Analyze Uploaded File**.

If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

18.1.4.3

AGTW – Logging On to the Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.

2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.

3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.

4. In the **Category** navigation pane, click **Session**.

5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter the applicable terminal server address:

- For Primary/Location A MSO Terminal Server: 10.<Z0>233.222
- For Secondary/ Location B MSO Terminal Server: 10<Z0>233.223
- For Console/DCS Site Terminal Server: 10.<Z0>.SITE.51

 **NOTE:** For Remote Control Sites, Terminal Server is optional.

- For BTS/Wave sites: 10.<Z0>127.SITE.51

where <Z0> is the zone octet where the terminal server is located.



IMPORTANT: S-DCS racks are normally custom-built and may not have a Terminal Server.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: `motorola`
8. At the prompt, enter the password.
9. Select the option associated with the **Dispatch Communications Server** to which you want to log in.
10. At the logon prompt, enter: `sysadmin`
11. At the prompt, enter the current password.

The **System Administrator Main Menu** appears.
12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.
14. At the logon prompt, enter: `agtwdadmin`

The server application menu appears.

18.1.4.4

AGTW – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: `y`

A message appears showing that the application server is disabled.
5. Enter `q` twice to go back to the **Application Servers Status Administration** menu.

18.1.4.5

AGTW – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

The file names of the backup files are read on the default storage for each application.

If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.

4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named **zoneXX.nmdYYY_agtwdb_ZZ_timestamp**, where XX is the zone ID, ZZ is a number in the interval 01-05, YYY is a number in the interval 1-230, and timestamp is a date and time written as one row of digits with the format yyymmddhhmm.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

18.1.4.6

AGTW – Enabling the Application Server

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu
-----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

2. Enter the number for **Application Servers Status Administration**.

3. Enter the number for **Enable Application Servers**.

4. Enter the number for the application server you want to enable.
A message appears showing that the application server is enabled.
5. Enter: **q** twice to go back to the **Application Servers Status Administration** menu.

18.1.5

AGTW – Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server. See “Clearing the Node Secret for a Particular Node” in the *Network Security* manual.
2. If RSA Two-Factor Authentication is present in the system, install and configure the RSA software. For detailed procedures, see “Installing and Configuring the RSA Authentication on Linux Devices” in the *Network Security* manual.

 **IMPORTANT:** When restoring a physical server hosting multiple virtualized applications, you should install RSA software once for **all** Linux applications. Because ESU framework handles the installation, ensure you restore and configure all Linux applications before installing RSA software.

18.1.6

AGTW – Post-Restoration Checks

Procedure:

1. Check that the AGTW Server Application is running. To do this, list the active processes using the **ps** command and search for an **agtw** process.
2. Check that the **/var/log/messages** folder contains a startup message.

An example startup message:

```
Aug 30 14:24:46 zdk02lix10-vm agtw[20096]: TIMESTAMP:2011-08-30  
14:24:46.235627 SOURCE:agtw.CAudioGateway LEVEL:LOG_INFO LOCATION:.../agtw.cpp(115)  
MESSAGE:Version: AGTW_D00.00.00.01
```

3. Check that the AGTW Server is connected to the CCE Server. To do this, check the log file in **/var/log/messages** folder. If the connection is set up a message similar to the one below will be there:

```
Aug 30 14:26:09 zdk02lix10-vm agtw[20096]: TIMESTAMP:2011-08-30 14:26:09.665863  
SOURCE:agtw.CAppLayer LEVEL:LOG_INFO LOCATION:.../applayer.cpp(544) MESSAGE:Link  
status 0: Link Active Up
```

4. Use the **netstat** command to check that port 58302 is open.

18.1.7

AGTW – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

18.1.7.1

AGTW – Starting Up the Upgrade Console

Prerequisites:

Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>

**IMPORTANT:**

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.

3. In the **Password** field, type the password related to the user name.

4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

18.1.7.2

AGTW – Configuring a Backup

Prerequisites:

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **agt01**, **agt02**, **agt03**, **agt04** or **agt05** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the AGTW application in the correct zone.



NOTE: You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **agt01**, **agt02**, **agt03**, **agt04** or **agt05** application in the **Use Central Storage** column. Make sure that you select the check box for the AGTW in the correct zone.

4. If you want to save the backup file in the Storage PC, select the check box of the **agt01**, **agt02**, **agt03**, **agt04** or **agt05** application in the **Use Storage PC** column.



NOTE: The backup file will be saved on all Storage PCs.

5. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [AGTW – Backing Up Data On-Demand on page 299](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [AGTW – Scheduling Backup on page 300](#).
- You can do both.



IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

18.1.7.3

AGTW – Backing Up Data On-Demand

Prerequisites:

Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **agt01**, **agt02**, **agt03**, **agt04** or **agt05** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [AGTW – Scheduling Backup on page 300](#).
- If you want to save the backup file on the NM Client PC, continue to [AGTW – Downloading a Backup File to the NM Client PC on page 300](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

18.1.7.4

AGTW – Scheduling Backup

Prerequisites:

Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.
A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.
2. Click **New**.
A page appears allowing you to define the scheduled backup.
3. Do the following:
 - a. In the **Name** field, type a name for the scheduled backup task.
 - b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.
 - c. In the **Day** drop-down list, select a week day or select **DAILY**.
 - d. In the **Hour** drop-down list, select at which hour the backup must run.
 - e. In the **Minute** drop-down list, select at which minute the backup must run.
 - f. Click **Submit**.A list appears in which you must click **Select** in the row containing the **agt01**, **agt02**, **agt03**, **agt04** or **agt05** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time. You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.
4. If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [AGTW – Downloading a Backup File to the NM Client PC on page 300](#). Otherwise, you do not have to do anything else regarding backup.

Postrequisites:

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

18.1.7.5

AGTW – Downloading a Backup File to the NM Client PC

Prerequisites:

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.



IMPORTANT: The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Save**.

3. In the **Save As** window, select a location for the file and click **Save**.

18.2

Call Control Entity (CCE) Software Application Restoration

Table 66: Call Control Entity (CCE) Server – Backup and Restoration Checklist

Action	Reference	Done
Restoring the application	CCE – Restoration Impact on page 301 CCE – Pre-Restoration Checks on page 302 CCE – Restoring Application on page 303 CCE – Application Configuration on page 302 CCE – Restoring Data from Backup on page 305 CCE – Installing and Configuring RSA Authentication Software on page 309 CCE – Post-Restoration Checks on page 311	
Backing up the application	CCE – Backing Up Data on page 311	

18.2.1

CCE – Restoration Impact

Table 67: CCE – Restoration Impact

Action	Service Affected	Service Downtime
CCE Server Restoration	<p>During the CCE Server restoration all connections from external clients are lost (for each CCE Server that is being restored).</p> <p>As a result:</p> <ul style="list-style-type: none"> • all calls ongoing when restoration starts, are stopped • no new calls can be started. 	for the duration of the restoration

Action	Service Affected	Service Downtime
CCE Server Restoration	Each CCE Server that is being restored loses connectivity with the Fault Management system. As a result faults showing that the CCE Server is down or unreachable might appear in the Fault Manager application.	for the duration of the restoration
CCE Server Restoration	The Audio Gateway (AGTW) Server also loses connectivity to the CCE Server that is being restored. As a result the AGTW Server will alert the Fault Manager application, that the link with CCE Server has been lost.	for the duration of the restoration
Operating System Restoration	OS restoration by default cleans out the database. As a result after OS restoration the database needs to be restored from backup.	for the duration of the restoration

18.2.2

CCE – Pre-Restoration Checks

Before you start the restoration, perform the following actions:

Procedure:

1. Stop all ongoing calls and all remote connections to the CCE Server.
2. Stop all console services running on the CCE Server. After stopping the console services, check the Windows Event Viewer logs for any unknown errors.

If there are no unknown errors, proceed to the next step. If errors appear – reboot the CCE Server, stop the console services (they are automatically started on each reboot) and check again. If errors still appear, contact your Motorola Solutions Support team.



IMPORTANT: Save the Windows Event Viewer log for inspection by the Support team.

3. Optional: If the database needs to be restored as well, empty the database folder. The database folder to be emptied is: C:\ProgramData\Motorola MCC7500DCS\Datasets



NOTE: If you are restoring the OS, the database will be cleaned out by default.

18.2.3

CCE – Restoring Software

18.2.3.1

CCE – Application Configuration

Once the CCE Server is installed it is ready to operate. No additional configuration of the CCE Server software is needed.

The CCE Server is an Application Server installed on the MCC 7500 Dispatch Communications Server (DCS). For the MCC 7500 DCS to be fully operational:

- Both the Call Control Entity (CCE) Server and the Audio Gateway (AGTW) Server applications need to be installed on the MCC 7500 DCS.
- The DCS needs to be configured in the Zone Configuration Manager (ZCM) application.
- The CRAM Service needs to be configured when the DCS is started for the first time.

For more information on backup and restore procedures for the AGTW Server, see [Audio Gateway \(AGTW\) Software Application Restoration on page 291](#).

The configuration of the MCC 7500 DCS in the Zone Configuration Manager (ZCM) application includes the following objects:

- Dispatch Communications Server Application object
- Speaker Channel object

For more information on configuring these objects, see the *Zone Configuration Manager* manual.

For information on configuring the CRAM Service on the DCS, see the *MCC 7500 Dispatch Communications Server* manual.

18.2.3.2

CCE – Restoring Application

Prerequisites:

Log on to iGAS as `instadm`. Depending on the access method, see one of the following procedures:

- [Logging On to iGAS Through a Terminal Server on page 45](#)
- [Logging On to iGAS Through a KVM Switch on page 48](#)

Procedure:

1. At logon as `instadm`, verify that the **Installation Administrator Main Menu** appears:

```
Installation Administrator Main Menu -----
1. Reinstall Applications 2. View Installation Information 3. View Installation Log
4. License Administration 5. Load software from DVD 6. Application DVD Management
7. Application Device Management 8. Change password 9. Security Update Services
Management Please enter selection (1-9, q) [q]:
```

2. Enter the number for **Reinstall Applications**.

The list of available applications residing on the server appears.

3. Enter: `y` when the installer prompts you to re-install **CCE Server** and enter: `n` for other applications.

The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

4. Log off from the server by entering `q`
5. Log on to the server using the `sysadmin` logon and password.

The **System Administrator Main Menu** appears.

```
System Administrator Main Menu -----
1. Enable all Application Servers
2. Disable all Application Servers
3. Display Status of all Application Servers
4. Unix Administration
5. Application Servers Administration Menus
6. Application Servers Boot/Reboot/Shutdown
```

```
7. Application Servers Status Administration
8. Application Isolation Management
Please enter selection (1-8, q) [q]:
```

6. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

The **Application Servers Boot/Reboot/Shutdown** menu appears.

```
Application Servers Boot/Reboot/Shutdown -----
1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
Servers Please enter selection (1-3, q) [q]:
```

7. Enter the number for **Boot Application Servers**.

The **Boot Application** menu appears.

8. Enter the number for **CCE Server**.

You have booted the application. The **Application Servers Boot/Reboot/Shutdown** menu appears.

9. Enter: q and repeat this sequence until you log off from the server.

18.2.4

Backing Up CRAM Configuration



NOTE: For CRAM non-SSL, you must back up only the CRAM configuration settings.

Procedure:

1. Connect to the CCE through Remote Desktop Connection.
2. Open the **Registry Editor** by selecting **Start** → **Run**, and enter: `regedit`
3. In the **Registry Editor**, navigate to
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Motorola\Console\Cramp.
4. In the registry tree on the left, right-click **Cramp**. From the list of available options, select **Export**.
5. In the **Export Registry File** window, navigate to the location where you want to save the CRAM configuration settings, and type a name for the registry file. Click **Save**.
The registry settings are exported to the file you specified and the file is saved to the selected location.
6. For CRAM SSL, back up the certificate files listed in the following table:

Table 68: CRAM SSL—Certificate Files to Back Up

 **NOTE:** The following locations are the default ones. You can find the location you are using in the Remote API Configurator.

File Name	Location
server-cert.pem	C:\Program Files (x86)\Motorola\Dimetra\CRAM\<version>\Keys\output
server-key.pem	C:\Program Files (x86)\Motorola\Dimetra\CRAM\<version>\Keys\output
cacert.pem	C:\Program Files (x86)\Motorola\Dimetra\CRAM\<version>\Keys\output

18.2.5

CCE – Restoring Data from Backup

18.2.5.1

CCE – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open the web browser and enter the following URL address: <https://master-uis.ucs/ui>
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to [CCE – Uploading a Backup File to UIS on page 305](#). If the backup file is already in the UIS backup storage, continue to logging on to the server.

18.2.5.2

CCE – Uploading a Backup File to UIS

Prerequisites: Log on to the Upgrade Console with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the Upgrade Console.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.

 **NOTE:** If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Upload Files**.

The **Upload Files** screen appears.

2. Click **Browse**.

3. In the window that appears, select your backup file. Click **OK**.

 **NOTE:** The backup file is named `zone<XX>.nmd<YY>_ccedb_<ZZ>_<timestamp>`, where `<XX>` is the zone ID, `<ZZ>` is a number in the interval 01-05, `<YY>` is a number in the interval 1-230, and `<timestamp>` is a date and time written as one row of digits with the format `<yyyyymmddhhmm>`.

The name of the selected file appears in the **File Name** field.

4. Click **Upload**.

5. Click **Analyze Uploaded File**.

If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

18.2.5.3

CCE – Logging On to the Server

Prerequisites: Ensure that the server is operational.

Procedure:

1. Start PuTTY.
2. In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter the applicable terminal server address:

- For Primary/Location A MSO Terminal Server: 10.<Z0>233.222
- For Secondary/ Location B MSO Terminal Server: 10<Z0>233.223
- For Console/DCS Site Terminal Server: 10.<Z0>.SITE.51



NOTE: For Remote Control Sites, Terminal Server is optional.

- For BTS/Wave sites: 10.<Z0>127.SITE.51

where <Z0> is the zone octet where the terminal server is located.



IMPORTANT: S-DCS racks are normally custom-built and may not have a Terminal Server.

At the first attempt to log on, the **PuTTY Security Alert** window appears.

For details on messages appearing when establishing the SSH session, see [Messages Appearing when Establishing a Secure Session on page 46](#).

6. In the **PuTTY Security Alert** window, perform one of the actions:
 - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
 - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
7. At the logon prompt, enter: **motorola**
8. At the prompt, enter the password.
9. Select the option associated with the **Dispatch Communications Server** to which you want to log in.
10. At the logon prompt, enter: **sysadmin**
11. At the prompt, enter the current password.
The **System Administrator Main Menu** appears.
12. Enter the number for **Application Servers Administration Menus**.
13. Enter the number for the application server you want to log on to.

18.2.5.4

CCE – Disabling the Application Server

Prerequisites:

You must be logged on the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

1. Enter the number associated with **Application Servers Status Administration**.
2. Enter the number associated with **Disable Application Servers**.
3. Enter the number associated with the application server that you want to disable.
4. If prompted for confirmation, enter: y
A message appears showing that the application server is disabled.

5. Enter q twice to go back to the **Application Servers Status Administration** menu.

18.2.5.5

CCE – Restoring Data from Backup

Prerequisites:

You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.
A table appears, showing available backup files for applications in the different zones.
2. Click **Refresh File name**.
The file names of the backup files are read on the default storage for each application.
If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup files.
4. In the **Action** column for the backup file and application, click **Run**.

 **NOTE:** The backup file is named **zoneXX.nmdYYY_ccedb_ZZ_timestamp**, where XX is the zone ID, ZZ is a number in the interval 01-05, YYY is a number in the interval 1-230, and timestamp is a date and time written as one row of digits with the format yyyyymmddhhmm.

A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.
An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.

 **NOTE:** The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

18.2.5.6

Restoring CRAM Service Configuration

Procedure:

1. Connect to the CCE through Remote Desktop Connection.
2. Navigate to the registry settings backup file you created in [Backing Up CRAM Configuration on page 304](#).
3. Double-click the file.
4. In the dialog box verifying that you want to add the CRAM configuration settings to the registry, click **Yes**.

The CRAM configuration settings are added to the registry.

5. Close the confirmation message dialog box by clicking **OK**.

 **NOTE:** If you want to configure new CRAM settings in the Remote API Configurator, see "Remote API Configurator" in the MCC 7500 Dispatch Communications Server manual.

6. For CRAM SSL, copy the backed up certificate and key files back to their original locations.

For a list of files, see [Backing Up CRAM Configuration on page 304](#). For the file locations, see the Remote API Configurator.

 **IMPORTANT:** For CRAM SSL, verify that MCC7500 Services account has read permissions for the location of the restored certificate and key files. See [Enabling the Read Permissions for CRAM SSL on page 308](#).

18.2.5.7

Enabling the Read Permissions for CRAM SSL

This procedure describes how to verify that MCC7500 Services account has read permissions for the location of the restored certificate and key files for CRAM.

Procedure:

1. Open **File Explorer**, navigate to the location where certificates were restored, and right-click the folder containing certificates.
2. Select **Properties** and navigate to the **Security** tab.
3. Perform one of the following actions:

If...	Then...
If the "Users" group is present on the "Group or user names" list and "Read" is allowed for this group,	close the Properties window.

If...	Then...
If the "Users" group is not present on the "Group or user names" list, or "Read" is not allowed for this group,	<p>perform the following actions:</p> <ol style="list-style-type: none"> Click Edit.... In the Permissions window, click Add.... In the Select Users or Groups, in the dialog box, enter MCC7500 Services Click Check Names. Click OK. In the Permissions window, verify if the Allow is set to Read for the <MCC7500 Services> user. Click OK. Click OK again.

18.2.5.8

CCE – Enabling the Application Server

Prerequisites:

You must be logged in to the server, and the **System Administrator Main Menu** must be shown on your screen.

Procedure:

- Enter the number for **Application Servers Status Administration**.
- Enter the number for **Enable Application Servers**.
- Enter the number for the **Call Control Entity** application server.
 A message appears stating that the application server is enabled.
- Enter: **q** twice to go back to the **Application Servers Status Administration** menu.

18.2.6

CCE – Installing and Configuring RSA Authentication Software

Procedure:

- Clear 2FA Secret key on the RSA server. See the *Network Security* manual.
- Install and configure the RSA software. For more information, see the *Network Security* manual.



IMPORTANT:

When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

The RSA Agent installation should be performed after the promoting of Domain Controller.

18.2.7

CCE – Verifying Service Startup Type

After each installation, ensure that the CCE services are initiated at system start.

Procedure:

1. Log on to the CCE. See [Accessing Virtual Machines with the Web-Based Client on page 310](#).
2. In the **Search Windows** search box, enter: services.msc
3. If prompted if you want to allow the program to make changes to the computer, select **Yes**.
4. Ensure that the **Dimetra Console Boot Manager** service is loaded at system start:
 - a. In the **Services** window, double-click the service
 - b. In the **Dimetra Console Boot Manager Properties (Local Computer)** window, **General** tab, ensure that the **Startup type** is set to automatic.
 - c. Click **OK**.
5. Ensure that the **Dimetra Console Agent Manager** service is loaded at system start:
 - a. In the **Services** window, double-click the service
 - b. In the **Dimetra Console Agent Manager Properties (Local Computer)** window, **General** tab, ensure that the **Startup type** is set to automatic.
 - c. Click **OK**.
6. In the **Services** window, locate the **Dimetra Console Remote API Manager** is loaded at system start:
 - a. In the **Services** window, double-click the service
 - b. In the **Dimetra Console Remote API Manager Properties (Local Computer)** window, **General** tab, ensure that the **Startup type** is set to automatic
 - c. Click **OK**.
7. In the **Services** window, locate the **SNMP Trap** is loaded at system start:
 - a. In the **Services** window, double-click the service
 - b. In the **SNMP Trap properties (Local Computer)** window, **General** tab, ensure that the **Startup type** is set to automatic
 - c. Click **OK**.
8. Reboot the Dispatch Communications Server.

18.2.7.1

Accessing Virtual Machines with the Web-Based Client

Procedure:

1. Open a web browser (Chromium).
2. In the address field, enter the IP address of the HostOS you want to access.
3. Perform the following actions:
 - a. In the **User name** field, enter: sysadmin
 - b. In the **Password** field, enter the password.
 - c. Click **Log in**.
4. In the Web-based client, perform the following actions:

- a. In the **Navigator** pane, click **Virtual Machines** .



NOTE: If a red exclamation mark is visible next to **System Time information** under the **System** tab in the **Navigator**, you can ignore it. To verify system time synchronization status, you can log in to IGAS as **sysadmin** user and use the **NTP Administration** menu.

- b. On the **Virtual Machines** list, select the check box next to the Virtual Machine you want to access.
- c. Select the **Consoles** tab.
- d. In the **Console Type** section, select **VNC** .



IMPORTANT: Do not use other console types.

The graphical console appears in a new window.



NOTE: If a VNC connection to virtual machine in Cockpit fails to pass keystrokes, you can press **CTRL+ALT+DEL** , and fold and unfold the virtual machine bar.



NOTE: After a fresh installation or upgrade of CCE on DCS server, an unexpected Microsoft Windows dialog box appears, prompting you to restart your computer to apply the changes. You can ignore it or click **Restart Later**.

18.2.8

CCE – Post-Restoration Checks

Once the restoration is complete, follow the steps below to ensure it was successful.

Process:

1. Log on to the CCE. See [Accessing Virtual Machines with the Web-Based Client on page 310](#).
2. Check the Windows Event Viewer log for any unknown errors. If there are any errors in the Windows Event Viewer log, contact your Motorola Solutions support team.
3. If the Audio Gateway (AGTW) Server is already installed, verify that the AGTW Server has connectivity to the CCE Server. To do this, find the following entry in the Windows Event Viewer log:

Event ID == 82

The LLP process has alerted the AudioManager that the AGTW link is up.

If there is no such entry in the Event Viewer, the link with the AGTW is down or incorrectly configured.

18.2.9

CCE – Backing Up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you create the backup, you need to configure it.

18.2.9.1

CCE – Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open an Internet browser and enter the following URL address: <https://master-uis.ucs/ui>

**IMPORTANT:**

You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

- For MUIS01: <https://ucs-muis01.ucs/ui>
- For MUIS02: <https://ucs-muis02.ucs/ui>

2. In the **User name** field, type a user name associated with the **Backup** user role.

3. In the **Password** field, type the password related to the user name.

4. Click **Log in**.

You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

18.2.9.2

CCE – Configuring a Backup

Prerequisites:

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **cce01, cce02, cce03, cce04** or **cce05** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the CCE application in the correct zone.



NOTE: You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **cce01, cce02, cce03, cce04** or **cce05** application in the **Use Central Storage** column. Make sure that you select the check box for the CCE in the correct zone.

4. Click **Apply changes**.

The **Backup** page appears showing applications selected for backup.

Postrequisites:

You now have these possibilities:

- If you want to create a backup file immediately, continue to [CCE – Backing Up Data On-Demand on page 313](#).
- If you want to create a scheduled backup task running at regular intervals, continue to [CCE – Scheduling Backup on page 313](#).
- You can do both.

18.2.9.3

CCE – Backing Up Data On-Demand

Prerequisites:

Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **cce01**, **cce02**, **cce03**, **cce04** or **cce05** application in the relevant zone, click **Run**.

 **NOTE:** You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites:

You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to [CCE – Scheduling Backup on page 313](#).
- If you want to save the backup file on the NM Client PC, continue to [CCE – Downloading a Backup File to the NM Client PC on page 314](#).
- If the backup file you just created satisfies your needs for backup, you do not have to do anything else regarding backup.

18.2.9.4

CCE – Scheduling Backup

Prerequisites:

Before you can start this procedure, you must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have the backup configured in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

A page appears allowing you to define the scheduled backup.

3. Do the following:

- a. In the **Name** field, type a name for the scheduled backup task.

- b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

A list appears in which you must click **Select** in the row containing the **cce01**, **cce02**, **cce03**, **cce04** or **cce05** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.

- c. In the **Day** drop-down list, select a week day or select **DAILY**.
d. In the **Hour** drop-down list, select at which hour the backup must run.
e. In the **Minute** drop-down list, select at which minute the backup must run.
f. Click **Submit**.

You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

4. If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to [CCE – Downloading a Backup File to the NM Client PC on page 314](#). Otherwise, you do not have to do anything else regarding backup.

Postrequisites:

 **IMPORTANT:** If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise, the scheduled backup task for the application continues to run.

18.2.9.5

CCE – Downloading a Backup File to the NM Client PC

 **IMPORTANT:** If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Before you can start this procedure, you must be logged on to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

 **NOTE:** If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.
 **IMPORTANT:** The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.
A table appears, showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.
2. Click **Save**.
3. In the **Save As** window, select a location for the file and click **Save**.